Benutzeranwendung: Installationshandbuch

Novell®
Rollenbasiertes Bereitstellungsmodul für Identity Manager

4.0

15. Oktober 2010

www.novell.com

Rechtliche Hinweise

Novell, Inc. leistet keinerlei Gewähr bezüglich des Inhalts oder Gebrauchs dieses Handbuchs. Insbesondere werden keine ausdrücklichen oder stillschweigenden Gewährleistungen hinsichtlich der handelsüblichen Qualität oder Eignung für einen bestimmten Zweck übernommen. Novell, Inc. behält sich weiterhin das Recht vor, diese Dokumentation zu revidieren und ihren Inhalt jederzeit und ohne vorherige Ankündigung zu ändern.

Des Weiteren übernimmt Novell, Inc. für Software keinerlei Haftung und schließt insbesondere jegliche ausdrücklichen oder impliziten Gewährleistungsansprüche bezüglich der Marktfähigkeit oder der Eignung für einen bestimmten Zweck aus. Außerdem behält sich Novell, Inc. das Recht vor, Novell-Software ganz oder teilweise jederzeit inhaltlich zu ändern, ohne dass für Novell, Inc. die Verpflichtung entsteht, Personen oder Organisationen von diesen Überarbeitungen oder Änderungen in Kenntnis zu setzen.

Alle im Zusammenhang mit dieser Vereinbarung zur Verfügung gestellten Produkte oder technischen Informationen unterliegen möglicherweise den US-Gesetzen zur Exportkontrolle sowie den Handelsgesetzen anderer Länder. Sie erkennen alle Ausfuhrkontrollbestimmungen an und erklären sich damit einverstanden, alle für ausstehende Exporte, Re-Exporte oder Importe erforderlichen Lizenzen bzw. Klassifizierungen einzuholen. Sie erklären sich damit einverstanden, nicht an juristische Personen, die in der aktuellen US-Exportausschlussliste enthalten sind, oder an in den US-Exportgesetzen aufgeführte terroristische Länder oder Länder, die einem Embargo unterliegen, zu exportieren oder zu reexportieren. Sie stimmen zu, keine Lieferungen für verbotene nukleare oder chemisch-biologische Waffen oder Waffen im Zusammenhang mit Flugkörpern zu verwenden. Weitere Informationen zum Export von Novell-Software finden Sie auf der Webseite Novell International Trade Services (http://www.novell.com/info/exports/). Novell übernimmt keine Verantwortung für das Nichteinholen notwendiger Exportgenehmigungen.

Copyright © 2008, Novell, Inc. Alle Rechte vorbehalten. Ohne ausdrückliche, schriftliche Genehmigung des Herausgebers darf kein Teil dieser Veröffentlichung reproduziert, fotokopiert, übertragen oder in einem Speichersystem verarbeitet werden.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
USA.
www.novell.com

Online-Dokumentation: Die neueste Online-Dokumentation für dieses und andere Novell-Produkte finden Sie auf der Dokumentations-Webseite (http://www.novell.com/documentation) von Novell.

Novell-Marken

Hinweise zu Novell-Marken finden Sie in der Novell Trademark and Service Mark-Liste (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materialien von Drittanbietern

Die Rechte für alle Marken von Drittanbietern liegen bei den jeweiligen Eigentümern.

Inhalt

Informationen zu diesem Handbuch 9

1 Überblick über die Installation des rollenbasierten Bereitstellungsmoduls 11

1.1 Installations-Checkliste . . . 11
1.2 Allgemeines zum Installationsprogramm . . . 12
1.3 Systemanforderungen . . . 12

2 Voraussetzungen 17

2.1 Installation des Identity Manager-Metaverzeichnisses . . . 17
2.2 Herunterladen des rollenbasierten Bereitstellungsmoduls . . . 17
2.3 Installation eines Anwendungsservers . . . 19
2.3.1 Installation des JBoss-Anwendungsservers . . . 19
2.3.2 Installation des WebLogic-Anwendungsservers . . . 25
2.3.3 Installation des WebSphere-Anwendungsservers . . . 25
2.4 Installieren einer Datenbank . . . 26
2.4.1 Hinweise zum Konfigurieren einer MySQL-Datenbank . . . 26
2.4.2 Hinweise zum Konfigurieren einer Oracle-Datenbank . . . 28
2.4.3 Hinweise zum Konfigurieren einer MS SQL Server-Datenbank . . . 29
2.4.4 Hinweise zum Konfigurieren einer DB2-Datenbank . . . 29
2.5 Installieren des Java Development Kit . . . 32

3 Installation des rollenbasierten Bereitstellungsmoduls 33

3.1 Installieren des rollenbasierten Bereitstellungsmoduls . . . 33
3.2 Ausführen des Dienstprogramms „NrfCaseUpdate“ . . . 34
3.2.1 Überblick über NrfCaseUpdate . . . 34
3.2.2 Installationsüberblick . . . 34
3.2.3 Wie sich „NrfCaseUpdate“ auf das Schema auswirkt . . . 35
3.2.4 Erstellen einer Sicherungskopie der Benutzeranwendungstreiber . . . 35
3.2.5 Verwenden von NrfCaseUpdate . . . 35
3.2.6 Verifizierung des „NrfCaseUpdate“-Prozesses . . . 38
3.2.7 Aktivieren der JRE für SSL-Verbindungen . . . 38
3.2.8 Wiederherstellen ungültig gemachter Benutzeranwendungstreiber . . . 39
3.3 Ausführen des RBPM-Installationsprogramms . . . 40
3.4 Schema manuell erweitern . . . 47

4 Erstellen der Treiber 49

4.1 Erstellen der Treiber in Designer . . . 49
4.1.1 Installieren der Pakete . . . 49
4.1.2 Erstellen des Benutzeranwendungstreibers in Designer . . . 51
4.1.3 Erstellen des Rollen- und Ressourcenservice-Treibers in Designer . . . 55
4.1.4 Bereitstellen der Treiber . . . 57

5 Installieren der Benutzeranwendung auf JBoss 59

5.1 Installieren und Konfigurieren der Benutzeranwendungs-WAR . . . 59
5.1.1 Anzeigen der Installations- und Protokolldateien . . . 79

5.2 Testen der Installation 79

6 Installieren der Benutzeranwendung auf WebSphere 81

6.1 Installieren und Konfigurieren der Benutzeranwendungs-WAR 81
6.1.1 Anzeigen der Installationsprotokolldateien 96
6.2 Konfigurieren der WebSphere-Umgebung 96
6.2.1 Konfiguration eines Verbindungspools 96
6.2.2 Hinzufügen von Benutzeranwendungs-Konfigurationsdateien und JVM-Systemeigenschaften 104
6.2.3 Importieren der eDirectory-Herkunftsverbürgung in den WebSphere-Keystore . . . 110
6.2.4 Übergeben der preferIPv4Stack-Eigenschaft an die JVM 111
6.3 Bereitstellung der WAR-Datei 111
6.3.1 Zusätzliche Konfiguration für WebSphere 7.0 112
6.4 Starten der und Zugriff auf die Benutzeranwendung 112

7 Installieren der Benutzeranwendung auf WebLogic 113

7.1 WebLogic-Installations-Checkliste 113
7.2 Installieren und Konfigurieren der Benutzeranwendungs-WAR 114
7.2.1 Anzeigen der Installations- und Protokolldateien 128
7.3 Vorbereiten der WebLogic-Umgebung 128
7.3.1 Konfiguration des Verbindungspools 128
7.3.2 Angeben von Speicherorten für die RBPM-Konfigurationsdateien 129
7.3.3 Entfernen von OpenSAML JAR-Dateien 131
7.3.4 Workflow-Plugin und WebLogic-Setup 131
7.4 Bereitstellen der Benutzeranwendungs-WAR-Datei 131
7.5 Zugriff auf die Benutzeranwendung 131

8 Installation von der Konsole aus oder mit einem einzigen Befehl 133

8.1 Installation der Benutzeranwendung von der Konsole aus 133
8.2 Installation der Benutzeranwendung mit einem einzigen Befehl 134
8.3 Ausführen des JBossPostgreSQL-Dienstprogramms im Automatik- oder im Konsolenmodus 145
8.4 Ausführen des RIS-Installationsprogramms im Automatik- oder im Konsolenmodus 146

9 Aufgaben nach Abschluss der Installation 149

9.1 Aufzeichnen des Master-Schlüssels 149
9.2 Konfiguration der Benutzeranwendung 149
9.2.1 Einrichten der Protokollierung 150
9.3 Konfiguration von eDirectory 150
9.3.1 Erstellen von Indizes in eDirectory 150
9.3.2 Installieren und Konfigurieren der SAML-Beglaubigungsmethode 150
9.4 Neukonfiguration der Benutzeranwendungs-WAR-Datei nach der Installation 152
9.5 Konfigurieren der externen Verwaltung „Passwort vergessen“ 152
9.5.1 Angabe einer externen WAR-Datei für die Verwaltung von „Passwort vergessen“ 153
9.5.2 Angeben einer internen Passwort-WAR-Datei 153
9.5.3 Testen der externen WAR-Konfiguration für „Passwort vergessen“ 153
9.5.4 Konfiguration der SSL-Kommunikation zwischen JBoss-Servern 154
9.6 Aktualisierung der Einstellungen für „Passwort vergessen“ 154
9.7 Sicherheitsüberlegungen 154
9.8 Erhöhen der IDM Java-Heap-Größe 154

9.9 Fehlersuche 155

A IDM Benutzeranwendung - Konfigurationsreferenz 157

A.1 Benutzeranwendung - Konfiguration: Standardparameter 157
A.2 Konfiguration der Benutzeranwendung: Alle Parameter 160

Informationen zu diesem Handbuch

In diesem Handbuch wird die Installation des funktionsbasierten Bereitstellungsmoduls für Novell Identity Manager 4.0 beschrieben. Es behandelt folgende Themen:

- Kapitel 1, „Überblick über die Installation des rollenbasierten Bereitstellungsmoduls“, auf Seite 11
- Kapitel 2, „Voraussetzungen“, auf Seite 17
- Kapitel 3, „Installation des rollenbasierten Bereitstellungsmoduls“, auf Seite 33
- Kapitel 4, „Erstellen der Treiber“, auf Seite 49
- Kapitel 5, „Installieren der Benutzeranwendung auf JBoss“, auf Seite 59
- Kapitel 6, „Installieren der Benutzeranwendung auf WebSphere“, auf Seite 81
- Kapitel 7, „Installieren der Benutzeranwendung auf WebLogic“, auf Seite 113
- Kapitel 8, „Installation von der Konsole aus oder mit einem einzigen Befehl“, auf Seite 133
- Kapitel 9, „Aufgaben nach Abschluss der Installation“, auf Seite 149
- Anhang A, „IDM Benutzeranwendung - Konfigurationsreferenz“, auf Seite 157

Zielgruppe

Dieses Handbuch richtet sich an Administratoren und Berater, die für die Planung und Implementierung des rollenbasierten Bereitstellungsmoduls für Identity Manager zuständig sind.

Rückmeldungen

Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation zu diesem Produkt. Bitte verwenden Sie die Benutzerkommentarfunktion unten auf der jeweiligen Seite der Online-Dokumentation oder wählen Sie www.novell.com/documentation/feedback.html, und geben Sie dort Ihre Kommentare ein.

Zusätzliche Dokumentation

Zusätzliche Dokumentation zu Identity Manager 4.0 finden Sie auf der Website zur Dokumentation für Identity Manager 4.0 (http://www.novell.com/documentation/idm40/index.html).

1 Überblick über die Installation des rollenbasierten Bereitstellungsmoduls

Dieser Abschnitt gibt einen Überblick über die einzelnen Schritte bei der Installation des rollenbasierten Bereitstellungsmoduls. Es werden u. a. folgende Themen erläutert:

- Abschnitt 1.1, „Installations-Checkliste“, auf Seite 11
- Abschnitt 1.2, „Allgemeines zum Installationsprogramm“, auf Seite 12
- Abschnitt 1.3, „Systemanforderungen“, auf Seite 12

Wenn Sie von einer früheren Version der Benutzeranwendung oder des rollenbasierten Bereitstellungsmoduls migrieren, lesen Sie das *Benutzeranwendung: Migrationshandbuch* (http://www.novell.com/documentation/idm40/index.html)

1.1 Installations-Checkliste

Sie müssen zum Installieren des rollenbasierten Bereitstellungsmoduls für Novell Identity Manager die folgenden Aufgaben durchführen:

- ❑ Vergewissern Sie sich, dass Ihre Software die Systemanforderungen erfüllt. Weitere Informationen hierzu finden Sie unter Abschnitt 1.3, „Systemanforderungen“, auf Seite 12.
- ❑ Laden Sie das rollenbasierte Bereitstellungsmodul für Identity Manager herunter. Weitere Informationen hierzu finden Sie unter Abschnitt 2.2, „Herunterladen des rollenbasierten Bereitstellungsmoduls“, auf Seite 17.
- ❑ Richten Sie die folgenden unterstützenden Komponenten ein:
  - ❑ Stellen Sie sicher, dass ein unterstütztes Identity Manager-Metaverzeichnis installiert ist. Weitere Informationen hierzu finden Sie unter Abschnitt 2.1, „Installation des Identity Manager-Metaverzeichnisses“, auf Seite 17.
  - ❑ Installieren und konfigurieren Sie einen Anwendungsserver. Weitere Informationen hierzu finden Sie unter Abschnitt 2.3, „Installation eines Anwendungsservers“, auf Seite 19.
  - ❑ Installieren und konfigurieren Sie eine Datenbank. Weitere Informationen hierzu finden Sie unter Abschnitt 2.4, „Installieren einer Datenbank“, auf Seite 26.
- ❑ Installieren Sie die Metaverzeichniskomponenten des rollenbasierten Bereitstellungsmoduls. Weitere Informationen hierzu finden Sie unter Kapitel 3, „Installation des rollenbasierten Bereitstellungsmoduls“, auf Seite 33.
- ❑ Erstellen Sie den Benutzeranwendungstreiber in Designer 4.0 für Identity Manager.
  - Weitere Informationen hierzu finden Sie unter Abschnitt 4.1, „Erstellen der Treiber in Designer“, auf Seite 49.
- ❑ Erstellen Sie den Rollen- und Ressourcenservice-Treiber in Designer 4.0 für Identity Manager.
  - Weitere Informationen hierzu finden Sie unter Abschnitt 4.1, „Erstellen der Treiber in Designer“, auf Seite 49

- ❑ Installieren und konfigurieren Sie die Novell Identity Manager-Benutzeranwendung. (Sie müssen das korrekte JDK installiert haben, bevor Sie das Installationsprogramm starten. Weitere Informationen hierzu finden Sie unter Abschnitt 2.5, „Installieren des Java Development Kit“, auf Seite 32.)

  Das Installationsprogramm kann auf drei Arten gestartet werden:

  - Über die grafische Benutzeroberfläche. Lesen Sie dazu Folgendes:
    - Kapitel 5, „Installieren der Benutzeranwendung auf JBoss“, auf Seite 59.
    - Kapitel 6, „Installieren der Benutzeranwendung auf WebSphere“, auf Seite 81.
    - Kapitel 7, „Installieren der Benutzeranwendung auf WebLogic“, auf Seite 113.
  - Über die Konsolenschnittstelle (Befehlszeile). Weitere Informationen hierzu finden Sie unter Abschnitt 8.1, „Installation der Benutzeranwendung von der Konsole aus“, auf Seite 133.
  - Automatische Installation. Siehe Abschnitt 8.2, „Installation der Benutzeranwendung mit einem einzigen Befehl“, auf Seite 134.
- ❑ Führen Sie die Aufgaben nach der Installation aus, wie in Kapitel 9, „Aufgaben nach Abschluss der Installation“, auf Seite 149 beschrieben.

Wichtig: Dieses Handbuch enthält keine Anweisungen zum Einrichten der Sicherheitsumgebung. Weitere Informationen zur Sicherheit finden Sie im Benutzeranwendung: Administrationshandbuch (http://www.novell.com/documentation/idm40/index.html).

1.2 Allgemeines zum Installationsprogramm

Das Installationsprogramm der Benutzeranwendung führt folgende Vorgänge durch:

- Festlegung einer vorhandenen Version eines zu verwendenden Anwendungsservers.
- Legt eine vorhandene Version einer zu verwendenden Datenbank fest, z. B. PostgreSQL, Oracle, DB2, Microsoft SQL Server oder MySQL. Die Datenbank speichert Anwendungsdaten und Konfigurationsinformationen der Benutzeranwendung.
- Konfiguration der JDK-Zertifikatsdatei, sodass die Benutzeranwendung (die auf dem Anwendungsserver ausgeführt wird) sicher mit dem Identitätsdepot und mit der Benutzeranwendung kommunizieren kann.
- Konfiguration und Bereitstellung der Java-WAR-Datei (Web Application Archive) für die Novell Identity Manager-Benutzeranwendung und den Application Server. Unter WebSphere und WebLogic müssen Sie die WAR-Datei manuell bereitstellen.
- Ermöglicht das Protokollieren über Novell- oder OpenXDAS-Audit-Clients, falls gewünscht.
- Ermöglicht das Importieren eines vorhandenen Master-Schlüssels zur Wiederherstellung einer bestimmten Installation des rollenbasierten Bereitstellungsmoduls und zur Unterstützung von Clustern.

1.3 Systemanforderungen

Für die Verwendung des rollenbasierten Bereitstellungsmoduls für Novell Identity Manager 4.0 benötigen Sie jeweils eine der unter Tabelle 1-1 aufgeführten erforderlichen Komponenten.

Tabelle 1-1 *Systemanforderungen*

Erforderliche Systemkomponente	Systemanforderungen
Metaverzeichnis	eDirectory 8.8.6 mit Identity Manager 4.0 Eine Liste der unterstützten Betriebssysteme finden Sie in der Dokumentation zu Identity Manager und eDirectory.
Anwendungsserver	Die Benutzeranwendung kann auf JBoss, WebSphere und WebLogic ausgeführt werden, wie unten beschrieben. Die Benutzeranwendung mit JBoss 5.1 erfordert JRE 1.6.0_20 von Sun und wird auf den folgenden Systemen unterstützt: ◆ Windows Server 2003 SP2 (nur 32 Bit) ◆ Windows Server 2008 R2 (nur 64 Bit) ◆ SUSE Linux Enterprise Server 10 SP3 (32 und 64 Bit) ◆ SUSE Linux Enterprise Server 11 (32 und 64 Bit) ◆ Red Hat Enterprise Linux 5.4 (32 und 64 Bit) ◆ Solaris 10 (32 und 64 Bit) Die Benutzeranwendung auf WebSphere 7.0 benötigt die IBM J9-VM (Build 2.4, J2RE 1.6.0) und Fix Pack 7. Sie wird auf den folgenden Plattformen unterstützt: ◆ Windows Server 2003 SP2 (nur 32 Bit) ◆ Windows Server 2008 R2 (nur 64 Bit) ◆ SUSE Linux Enterprise Server 10 SP3 (32 und 64 Bit) ◆ SUSE Linux Enterprise Server 11 (32 und 64 Bit) ◆ Red Hat Enterprise Linux 5.4 (32 und 64 Bit) ◆ AIX 5.3 (64 Bit nur mit Oracle 11g als Datenbank) ◆ Solaris 10 (32 und 64 Bit) Die Benutzeranwendung auf WebLogic 10.3 erfordert JRockit JVM 1.6.0_17 und wird auf diesen Plattformen unterstützt. ◆ Windows Server 2003 SP2 (nur 32 Bit) ◆ Windows Server 2008 R2 (nur 64 Bit) ◆ SUSE Linux Enterprise Server 10 SP3 (32 und 64 Bit) ◆ SUSE Linux Enterprise Server 11 (32 und 64 Bit) ◆ Red Hat Enterprise Linux 5.4 (32 und 64 Bit) ◆ Solaris 10 (32 oder 64 Bit) **Hinweis:** Die Benutzeranwendung unterstützt die Xen- und VMWare-Virtualisierung, solange das Gastbetriebssystem von der Benutzeranwendung unterstützt wird.

Erforderliche Systemkomponente	Systemanforderungen
Browser	Die Benutzeranwendung unterstützt Firefox und Internet Explorer, wie nachfolgend beschrieben. Firefox 3.6 wird in den folgenden Umgebungen unterstützt: ◆ Windows XP mit SP3 ◆ Windows Vista ◆ Windows 7 ◆ SUSE Linux Enterprise Desktop 11 ◆ SUSE Linux Enterprise Server 11 ◆ Novell OpenSuSE 11.2 ◆ Apple Mac Internet Explorer 8 wird in den folgenden Umgebungen unterstützt: ◆ Windows XP mit SP3 ◆ Windows Vista ◆ Windows 7 Internet Explorer 7 wird in den folgenden Umgebungen unterstützt: ◆ Windows XP mit SP3
Datenbankserver	Die folgenden Datenbanken werden mit JBoss 5.1.0 unterstützt: ◆ MS SQL 2008 ◆ MySQL Version 5.1 ◆ Oracle 11g ◆ PostgreSQL 8.4.3 Die folgenden Datenbanken werden mit WebSphere 7.0 unterstützt: ◆ DB2 9.5 ◆ MS SQL 2008 ◆ Oracle 11g ◆ PostgreSQL 8.4.3 Die folgenden Datenbanken werden mit WebLogic 10.3 unterstützt: ◆ MS SQL 2008 ◆ Oracle 11g ◆ PostgreSQL 8.4.3
Designer	Designer 4.0
OpenXDAS	OpenXDAS Version 0.8.345 Die folgenden Versionen von OpenXDAS werden für SLES10 benötigt: ◆ openxdas-0.8.351-1.1.i586.rpm ◆ openxdas-0.8.351-1.1.x86_64.rpm

Erforderliche Systemkomponente	Systemanforderungen
Domänendienste	OES 2 SP1 Domänendienste für Windows
Passwortverwaltung - Sicherheitsabfrage	NMAS Challenge Response Login Method Version: 2770 Build: 20080603 oder höher wird für die Sicherheitsabfragefunktion der Passwortverwaltung benötigt.

Voraussetzungen

2

In diesem Abschnitt werden die Softwarekomponenten beschrieben, die Sie installieren oder konfigurieren müssen, bevor Sie das rollenbasierte Bereitstellungsmodul für Identity Manager (RBPM) installieren können. Es werden u. a. folgende Themen erläutert:

- Abschnitt 2.1, „Installation des Identity Manager-Metaverzeichnisses“, auf Seite 17
- Abschnitt 2.2, „Herunterladen des rollenbasierten Bereitstellungsmoduls“, auf Seite 17
- Abschnitt 2.3, „Installation eines Anwendungsservers“, auf Seite 19
- Abschnitt 2.4, „Installieren einer Datenbank“, auf Seite 26
- Abschnitt 2.5, „Installieren des Java Development Kit“, auf Seite 32

2.1 Installation des Identity Manager-Metaverzeichnisses

Das rollenbasierte Bereitstellungsmodul der Version 4.0 muss mit Identity Manager 4.0 verwendet werden.

Anweisungen zur Installation von Identity Manager 4.0 finden Sie auf der Website zur Identity Manager-Dokumentation (http://www.novell.com/documentation/idm40/index.html).

2.2 Herunterladen des rollenbasierten Bereitstellungsmoduls

Sie können das rollenbasierte Bereitstellungsmodul für Identity Manager 4.0 von der Website Novell Downloads (http://download.novell.com/index.jsp) herunterladen. Laden Sie die `.iso`-Image-Dateien für Ihr Produkt herunter, wie in Tabelle 2-1 angezeigt.

Tabelle 2-1 *Die .iso-Download-Dateien*

Für dieses Produkt	Diese .iso-Datei herunterladen
Benutzeranwendung	`Identity_Manager_RBPM_4_0_0_User_Application.iso`
Komponenten des rollenbasierten Bereitstellungs-moduls für das Meta-verzeichnis	`Identity_Manager_RBPM_4_0_0_Driver_Install.iso`

Tabelle 2-2 beschreibt die Installationsdateien, die in den `.iso`-Dateien der Benutzeranwendung und dem rollenbasierten Bereitstellungsmodul enthalten sind.

Tabelle 2-2 *In den ISOs enthaltene Dateien und Skripte*

Datei	Beschreibung
`IDMProv.war`	Das WAR-Archiv des rollenbasierten Bereitstellungsmoduls. Sie enthält die Identity Manager-Benutzeranwendung mit den Rollen der Identitätsselbstbedienung und des rollenbasierten Bereitstellungsmoduls.
`IDMUserApp.jar`	Das Installationsprogramm der Benutzeranwendung.
`silent.properties`	Eine Datei, die die für eine automatische Installation erforderlichen Parameter enthält. Diese Parameter entsprechen den Installationsparametern, die Sie bei der Installation der GUI oder der Konsolenschnittstelle angegeben haben. Sie sollten diese Datei kopieren und anschließend den Inhalt an Ihre Installationsumgebung anpassen.
`JBossPostgreSQL.bin` oder `JBossPostgreSQL.exe`	Ein praktisches Dienstprogramm zum Installieren des JBoss-Anwendungsservers und der PostgreSQL-Datenbank.
`nmassaml.zip`	Enthält eine eDirectory-Methode zur Unterstützung von SAML. Nur erforderlich, wenn Sie Access Manager nicht verwenden.
`rbpm_driver_install.exe`	Windows-Installationsprogramm für die Metaverzeichniskomponenten des rollenbasierten Bereitstellungsmoduls (Rollen- und Ressourcenservice-Treiber, Benutzeranwendungstreiber und eDirectory-Schema).
`rbpm_driver_install_linux.bin`	Linux-Installationsprogramm für die Metaverzeichniskomponenten des rollenbasierten Bereitstellungsmoduls (Rollen- und Ressourcenservice-Treiber, Benutzeranwendungstreiber und eDirectory-Schema).
`rbpm_driver_install_solaris.bin`	Solaris-Installationsprogramm für die Metaverzeichniskomponenten des rollenbasierten Bereitstellungsmoduls (Rollen- und Ressourcenservice-Treiber, Benutzeranwendungstreiber und eDirectory-Schema).

Das System, auf dem Sie das rollenbasierte Bereitstellungsmodul für Identity Manager installieren, benötigt mindestens 320 MB verfügbaren Speicherplatz sowie freien Speicher für die unterstützenden Anwendungen (Datenbank, Anwendungsserver usw.). Das System benötigt nach und nach zusätzlichen Speicherplatz für die Aufnahme weiterer Daten, z. B. Datenbanken oder Anwendungsserverprotokolle.

Der Standardinstallationsspeicherort lautet wie folgt:

- Linux oder Solaris: `/opt/novell/idm`
- Windows: `C:\Novell\IDM`

Sie können ein anderes Standardinstallationsverzeichnis während der Installation auswählen, es muss jedoch bereits vor Beginn der Installation vorhanden und beschreibbar sein (im Falle von Linux oder Solaris muss es außerdem von Nicht-`Root`-Benutzern beschreibbar sein).

2.3 Installation eines Anwendungsservers

- Abschnitt 2.3.1, „Installation des JBoss-Anwendungsservers“, auf Seite 19
- Abschnitt 2.3.2, „Installation des WebLogic-Anwendungsservers“, auf Seite 25
- Abschnitt 2.3.3, „Installation des WebSphere-Anwendungsservers“, auf Seite 25

2.3.1 Installation des JBoss-Anwendungsservers

Wenn Sie den JBoss-Anwendungsserver verwenden möchten, können Sie Folgendes tun:

- Laden Sie den JBoss-Anwendungsserver herunter und installieren Sie ihn gemäß den Anweisungen des Herstellers. Unter Abschnitt 1.3, „Systemanforderungen“, auf Seite 12 finden Sie die unterstützte Version.
- Verwenden Sie das JBossPostgreSQL-Dienstprogramm, das mit dem Download des rollenbasierten Bereitstellungsmoduls bereitgestellt wird, um den JBoss-Anwendungsserver (und optional PostgreSQL) zu installieren. Anleitungen finden Sie in „Installation des JBoss Application Servers und der PostgreSQL-Datenbank“ auf Seite 19.

Starten Sie den JBoss-Server erst, nachdem Sie das rollenbasierte Bereitstellungsmodul für Identity Manager installiert haben. Das Starten des JBoss-Servers gehört zu den nach der Installation durchzuführenden Aufgaben.

Tabelle 2-3 *Empfohlene Mindestanforderungen für JBoss-Anwendungsserver*

Komponente	Empfehlung
RAM	Für den JBoss-Anwendungsserver sollten mindestens 512 MB RAM zur Verfügung stehen, wenn das rollenbasierte Bereitstellungsmodul für Identity Manager ausgeführt wird.
Port	8180 ist der Standardport für den Anwendungsserver. Notieren Sie den Port, den Ihr Anwendungsserver verwendet.
SSL	Aktivieren Sie SSL, wenn Sie beabsichtigen, eine externe Passwortverwaltung zu verwenden: ◆ Aktivieren Sie SSL für die JBoss-Server, auf denen Sie das rollenbasierte Bereitstellungsmodul für Identity Manager und die Datei `IDMPwdMgt.war` bereitstellen möchten. ◆ Stellen Sie sicher, dass der SSL-Port in Ihrer Firewall offen ist. Weitere Informationen zum Aktivieren von SSL finden Sie in Ihrer JBoss-Dokumentation. Informationen zur Datei `IDMPwdMgt.war` finden Sie unter Abschnitt 9.5, „Konfigurieren der externen Verwaltung „Passwort vergessen““, auf Seite 152 sowie im *Benutzeranwendung: Administrationshandbuch* (http://www.novell.com/documentation/idm40/index.html).

Installation des JBoss Application Servers und der PostgreSQL-Datenbank

Das JBossPostgreSQL-Dienstprogramm installiert den JBoss-Anwendungsserver und PostgreSQL auf Ihrem System. Dieses Dienstprogramm unterstützt keinen Konsolenmodus, sondern erfordert eine grafische Benutzeroberflächenumgebung.

Hinweis: Bevor Sie das RBPM JBossPostgreSQL-Installationsprogramm unter Windows 2008 ausführen, müssen Sie sich bei Ihrem Windows-Administrator nach der Passwortrichtlinie für Ihr System erkundigen. Die Passwortrichtlinie für Windows 2008 Server verlangt, dass ein Passwort einem bestimmten Regelsatz entspricht. Die Richtlinie kann beispielsweise verlangen, dass ein Passwort nicht-alphabetische Zeichen sowie Zeichen in Groß- und Kleinschreibung enthalten oder mindestens 8 Zeichen lang sein muss. Die Richtlinie kann vom Windows-Administrator geändert oder deaktiviert werden.

Installationsprogramm als root-Benutzer ausführen Sie müssen das Installationsprogramm als root-Benutzer ausführen.

So führen Sie das JBossPostgreSQL-Dienstprogramm aus:

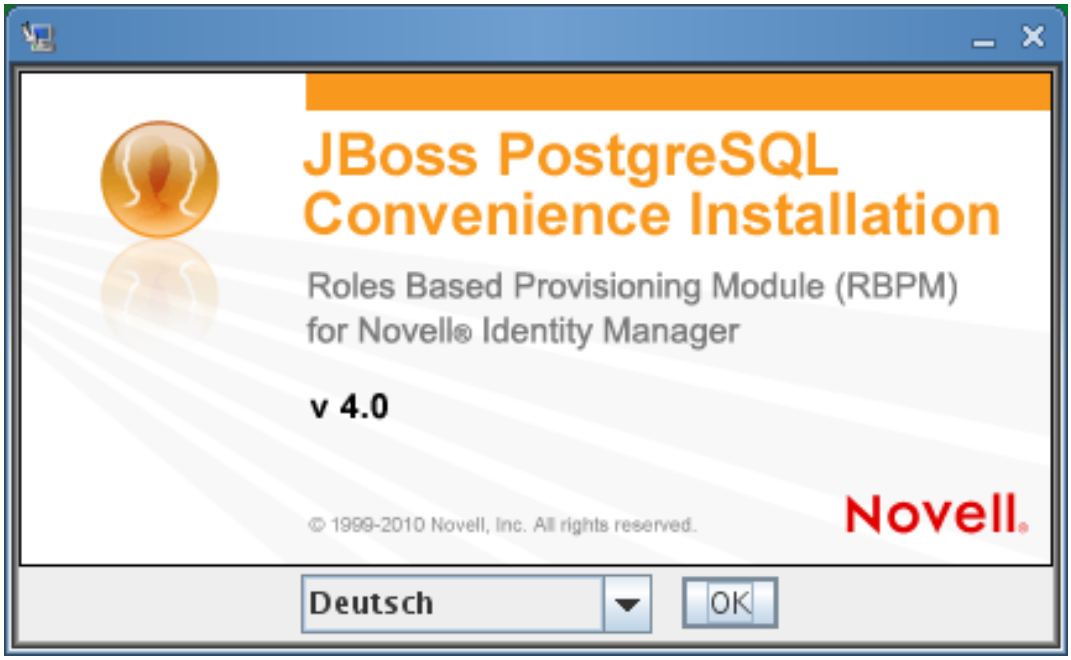
1 Suchen Sie die Datei `JBossPostgreSQL.bin` oder `JBossPostgreSQL.exe` in der .iso-Datei und führen Sie sie aus.

`/linux/jboss/JBossPostgreSQL.bin` (für Linux)

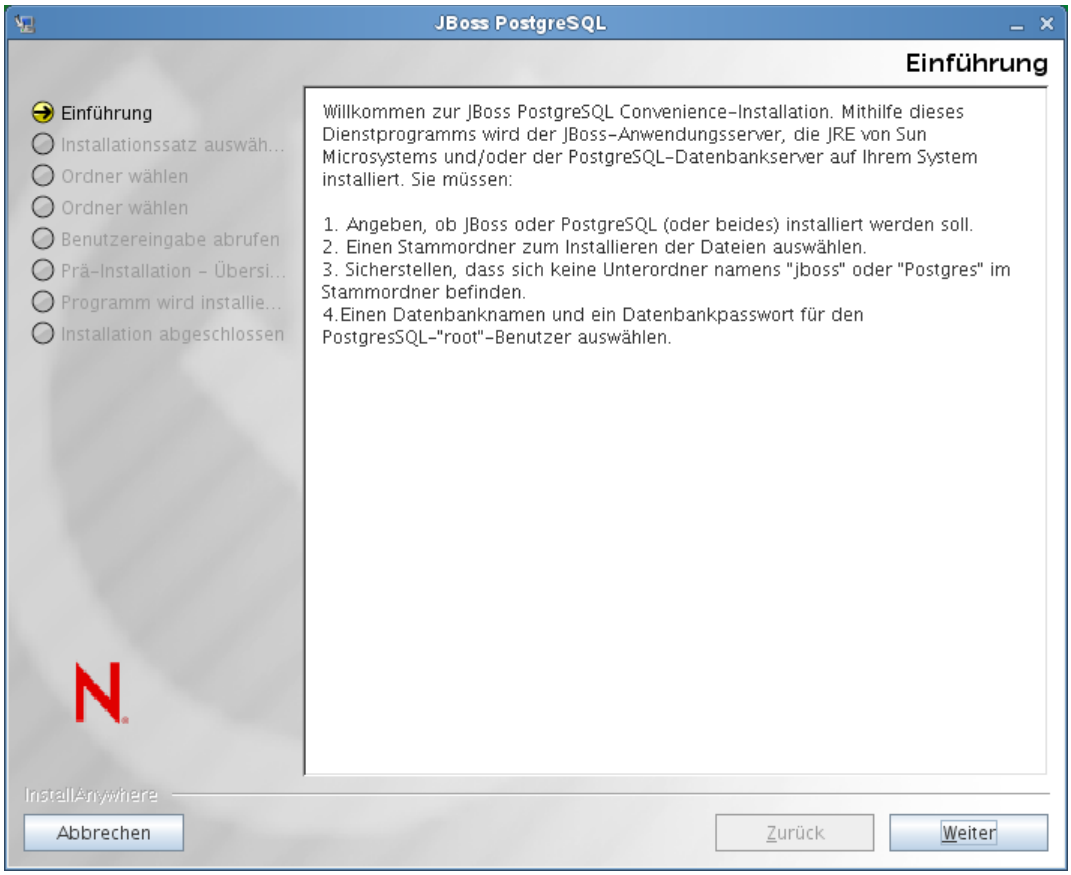
`/nt/jboss/JBossPostgreSQL.exe` (für Windows)

Das Dienstprogramm ist für Solaris nicht verfügbar.

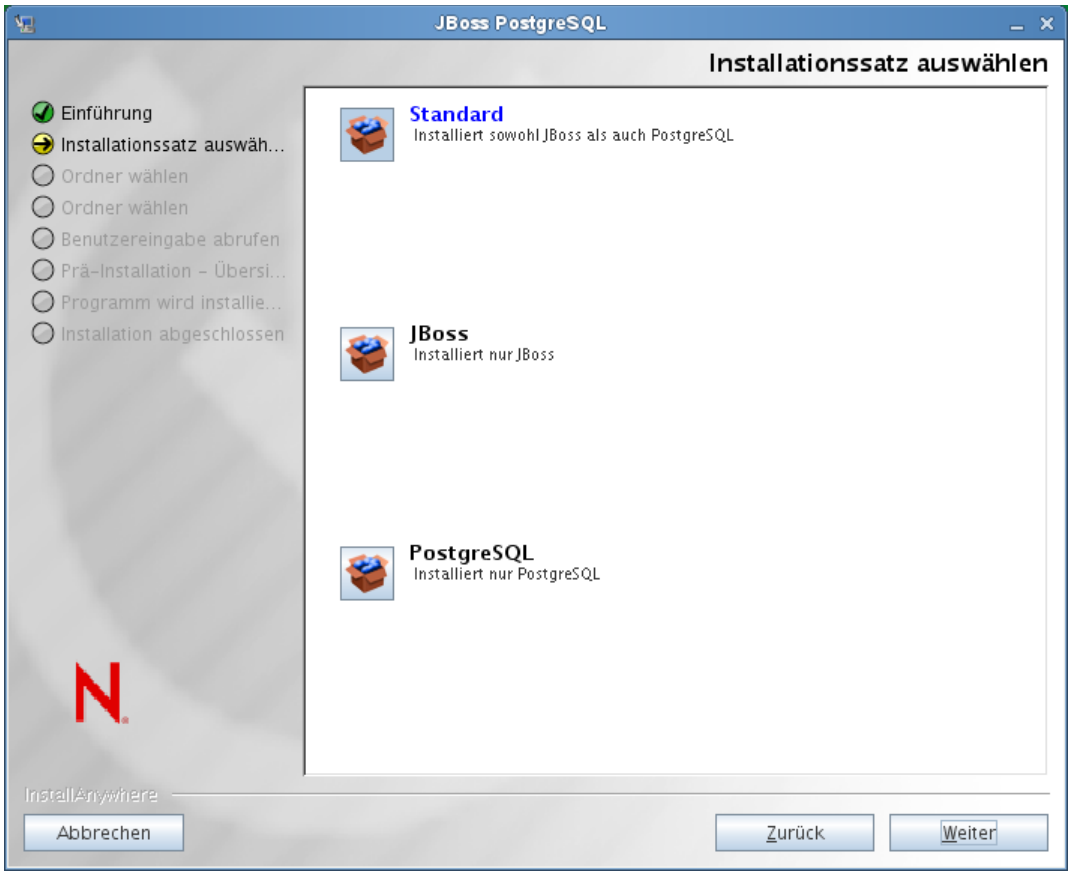
Der Eröffnungsbildschirm des JBossPostgreSQLJBossPostgreSQL-Dienstprogramms wird angezeigt:



Anschließend wird der Einführungsbildschirm angezeigt:

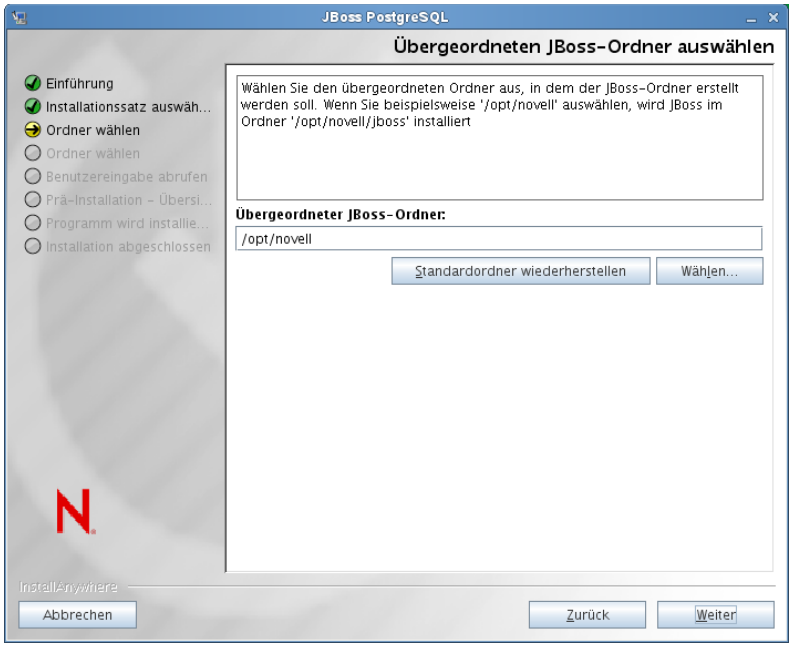
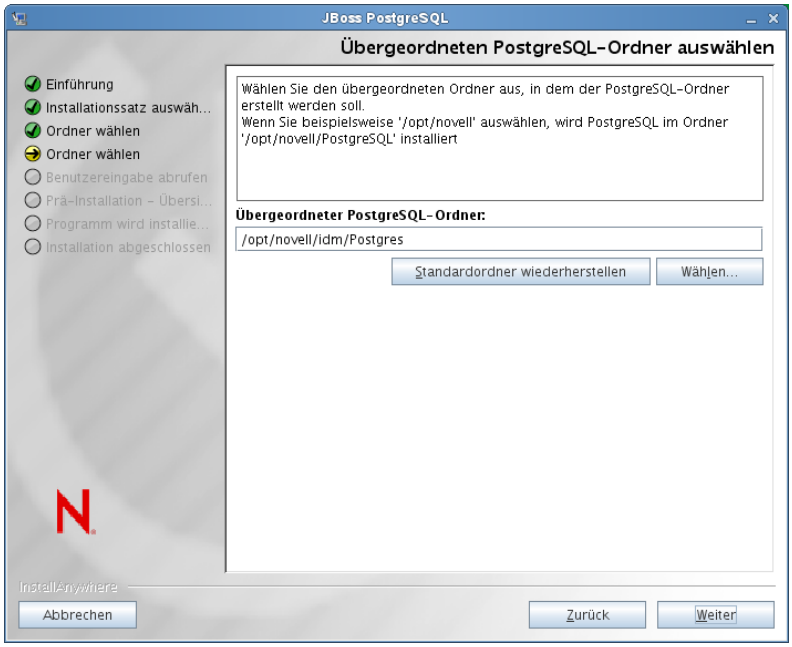

JBoss PostgreSQL
Einführung
Einführung
Installationssatz auswäh...
Ordner wählen
Ordner wählen
Benutzereingabe abrufen
Prä-Installation - Übersi...
Programm wird installie...
Installation abgeschlossen
Willkommen zur JBoss PostgreSQL Convenience-Installation. Mithilfe dieses Dienstprogramms wird der JBoss-Anwendungsserver, die JRE von Sun Microsystems und/oder der PostgreSQL-Datenbankserver auf Ihrem System installiert. Sie müssen:
1. Angeben, ob JBoss oder PostgreSQL (oder beides) installiert werden soll.
2. Einen Stammordner zum Installieren der Dateien auswählen.
3. Sicherstellen, dass sich keine Unterordner namens "jboss" oder "Postgres" im Stammordner befinden.
4.Einen Datenbanknamen und ein Datenbankpasswort für den PostgresSQL-"root"-Benutzer auswählen.
InstallAnywhere
Abbrechen
Zurück
Weiter

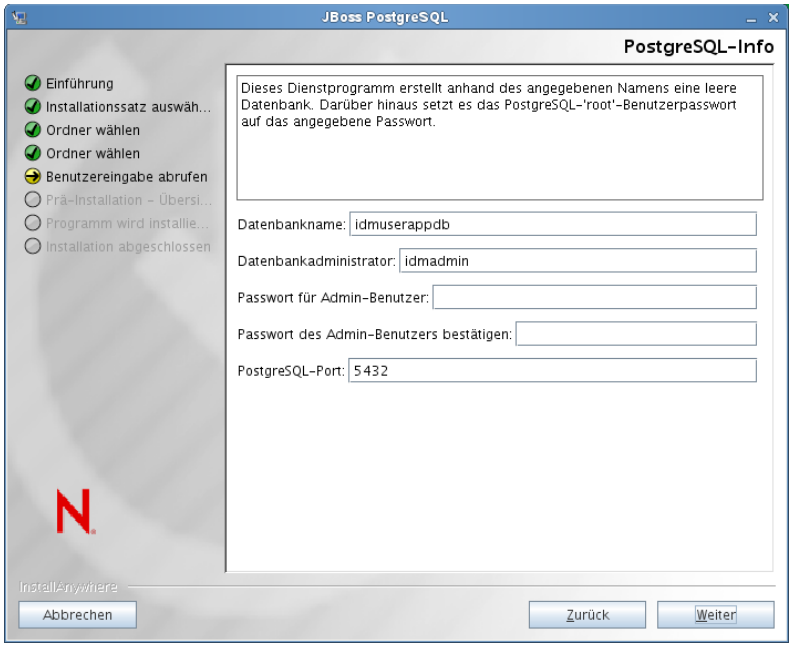
Wenn Sie auf „Weiter“ klicken, wird der Bildschirm *Installationssatz wählen* angezeigt:



2 Führen Sie zur Bedienung des Dienstprogramms die Anweisungen auf dem Bildschirm aus. Weitere Informationen hierzu finden Sie in der folgenden Tabelle.

Installationsbildschirm	Beschreibung
Auswählen des Installationssets	Wählen Sie die zu installierenden Produkte aus. ◆ *Standard:* JBoss und PostgreSQL einschließlich der Start- und Stopp-Skripts werden im von Ihnen angegebenen Verzeichnis installiert. ◆ *JBoss*: Installiert den JBoss-Anwendungsserver in das Verzeichnis, das Sie zusammen mit den Skripts zum Starten und Beenden angeben. **Hinweis:** Dieses Dienstprogramm installiert den JBoss-Anwendungsserver nicht als Windows-Dienst. Anleitungen finden Sie unter „Installieren des JBoss-Anwendungsservers als Dienst oder Daemon“ auf Seite 25. ◆ *PostgreSQL*: Installiert PostgreSQL und erstellt eine PostgreSQL-Datenbank zusammen mit den Skripts zum Starten und Beenden in dem Verzeichnis, das Sie angeben.

Installationsbildschirm	Beschreibung
Übergeordneten JBoss-Ordner auswählen	Klicken Sie auf *Auswählen*, um einen anderen Installationsordner als den Standardordner auszuwählen. 
Übergeordneten PostgreSQL-Ordner wählen	Klicken Sie auf *Auswählen*, um einen anderen Installationsordner als den Standardordner auszuwählen. 

Installationsbildschirm	Beschreibung
PostgreSQL-Info	Geben Sie hierzu Folgendes an: ◆ *Datenbankname*: Geben Sie den Namen der Datenbank für das zu erstellende Installationsprogramm an. Das Benutzeranwendungsinstallationsprogramm fragt Sie nach diesem Namen, daher sollten Sie sich den Namen und den Speicherort notieren. Die Standarddatenbank ist `idmadmin`. ◆ *Datenbankadministrator*: Der Benutzer wird der Administrator der Datenbank. Der Standardadministrator ist `idmuserappdb`. ◆ *Passwort für Admin-Benutzer*: Das Passwort des Datenbankadministrators. ◆ *Passwort des Admin-Benutzers bestätigen*: Bestätigung des Passworts. ◆ *PostgreSQL-Port*: Der Port, den der PostgreSQL-Datenbankserver überwacht. 
Zusammenfassung vor der Installation	Überprüfen Sie die Seite „Zusammenfassung“. Wenn die Spezifikationen korrekt sind, klicken Sie auf *Installieren*.

Installationsbildschirm	Beschreibung
Installation abgeschlossen	Nach der Installation der ausgewählten Produkte wird eine Meldung zur erfolgreichen Installation angezeigt: `The Installer has completed successfully. Thank you for choosing Novell` **Installationsprogramm erstellt novlua-Benutzer.** Das Installationsprogramm erstellt einen neuen Benutzer mit dem Namen „novlua“. Das jboss_init-Skript führt JBoss als dieser Benutzer aus und die definierten Berechtigungen in den JBoss-Dateien sind auf diesen Benutzer festgelegt. **Wichtig:** Bitte beachten Sie, dass das JBossPostgreSQL-Dienstprogramm weder die JMX-Konsole noch die JBoss-Webkonsole sichert. Somit bleibt die JBoss-Umgebung ganz offen. Sobald Sie die Installation abgeschlossen haben, müssen Sie die Umgebung schließen, um Sicherheitsrisiken auszuschließen.

Installieren des JBoss-Anwendungsservers als Dienst oder Daemon

Unter Linux startet JBoss standardmäßig als Dienst. Ein Skript mit dem Namen /etc/init.d/jboss_init start/stop wird installiert, damit JBoss beim Neustart des Systems gestartet wird.

Verwendung eines JavaServiceWrapper. Sie können mithilfe eines JavaServiceWrapper den JBoss-Anwendungsserver als Windows-Dienst installieren, starten und anhalten. Weitere Informationen hierzu finden Sie unter http://www.jboss.org/community/wiki/RunJBossAsAServiceOnWindows (http://www.jboss.org/community/wiki/RunJBossAsAServiceOnWindows). Ein derartiger Wrapper befindet sich unter http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html (http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html): Verwalten Sie Ihn mit JMX (siehe http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss (http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss)).

Wichtig: In früheren Versionen konnten Sie ein Dienstprogramm eines Drittanbieters, wie z. B. JavaService, verwenden, um den JBoss-Anwendungsserver als Windows-Dienst zu installieren, zu starten und anzuhalten, aber JBoss empfiehlt nicht mehr die Verwendung von JavaService. Einzelheiten finden Sie unter http://www.jboss.org/wiki/JavaService (http://www.jboss.org/community/wiki/JavaService).

2.3.2 Installation des WebLogic-Anwendungsservers

Wenn Sie den WebLogic-Anwendungsserver verwenden möchten, laden Sie ihn herunter und installieren Sie ihn. Unter Abschnitt 1.3, „Systemanforderungen“, auf Seite 12 finden Sie weitere Informationen zu den unterstützten Versionen.

2.3.3 Installation des WebSphere-Anwendungsservers

Wenn Sie den WebSphere Anwendungsserver verwenden möchten, laden Sie ihn herunter und installieren Sie ihn. Unter Abschnitt 1.3, „Systemanforderungen“, auf Seite 12 finden Sie weitere Informationen zu den unterstützten Versionen.

Hinweise zur DB2-Konfiguration finden Sie unter „Hinweise zum Konfigurieren einer DB2-Datenbank“ auf Seite 29.

2.4 Installieren einer Datenbank

Die Benutzeranwendung verwendet eine Datenbank für eine Reihe bestimmter Aufgaben, z. B. zum Speichern von Konfigurationsdaten und von Daten aus Workflow-Aktivitäten. Bevor Sie das rollenbasierte Bereitstellungsmodul und die Benutzeranwendung installieren können, müssen Sie eine der unterstützten Datenbanken für Ihre Plattform installiert und konfiguriert haben. Dies beinhaltet:

- ❑ Installieren Ihrer Datenbank und des Datenbanktreibers.
- ❑ Erstellen einer Datenbank oder einer Datenbankinstanz.
- ❑ Notieren der folgenden Datenbankparameter zur Verwendung in der Installationsprozedur für die Benutzeranwendung:
  - Host und Port
  - Datenbankname, Benutzername und Benutzerpasswort
- ❑ Erstellen einer Datenquelldatei, die auf die Datenbank zeigt.

  Die Methode variiert je nach Anwendungsserver. Für JBoss erstellt das Installationsprogramm für die Benutzeranwendung eine Anwendungsserver-Datenquelldatei, die auf die Datenbank verweist, und benennt die Datei anhand des Namens der WAR-Datei des rollenbasierten Bereitstellungsmoduls für Identity Manager. Für WebSphere und WebLogic müssen Sie die Datenquelle vor der Installation manuell konfigurieren.
- ❑ Datenbanken müssen für die Verwendung der Unicode-Kodierung aktiviert sein.

  Die Benutzeranwendung setzt voraus, dass der Zeichensatz der Datenbank die Unicode-Kodierung verwendet. So ist beispielsweise UTF-8 ein Zeichensatz, der die Unicode-Kodierung verwendet, Latin-1 hingegen verwendet keine Unicode-Kodierung. Stellen Sie vor der Installation der Benutzeranwendung sicher, dass Ihre Datenbank mit einem Zeichensatz konfiguriert wurde, der die Unicode-Kodierung verwendet.

Hinweis: Wenn Sie auf eine neue Version des rollenbasierten Bereitstellungsmoduls migrieren, müssen Sie die gleiche Benutzeranwendungsdatenbank verwenden, die Sie für die vorherige Installation verwendet haben (d. h. die Installation, von der aus Sie migrieren.)

2.4.1 Hinweise zum Konfigurieren einer MySQL-Datenbank

Die Benutzeranwendung erfordert die unten beschriebenen Konfigurationsoptionen für MySQL.

- „INNODB-Storage-Engine und Tabellentypen“ auf Seite 27
- „Zeichensatz“ auf Seite 27
- „Beachtung der Groß- und Kleinschreibung“ auf Seite 27
- „ANSI-Einstellung“ auf Seite 27
- „Benutzerkontoanforderungen“ auf Seite 28

INNODB-Storage-Engine und Tabellentypen

Die Benutzeranwendung verwendet die INNODB-Storage-Engine, sodass Sie INNODB-Tabellentypen für MySQL auswählen können. Wenn Sie eine MySQL-Tabelle erstellen, ohne den Tabellentyp anzugeben, wird der Tabelle standardmäßig der Tabellentyp „MyISAM“ zugeordnet. Sie können sicherstellen, dass Ihr MySQL-Server INNODB verwendet, indem Sie überprüfen, ob `my.cnf` (Linux oder Solaris) oder `my.ini` (Windows) die folgende Option enthält:

```
default-table-type=innodb
```

Die Option `skip-innodb` darf nicht enthalten sein.

Alternativ zum Festlegen der Option `default-table-type=innodb` können Sie die Option `ENGINE=InnoDB` an die „Create Table“-Anweisungen im SQL-Skript für Ihre Datenbank anhängen.

Zeichensatz

Legen Sie UTF-8 als Zeichensatz für den gesamten Server oder nur für eine Datenbank fest. Legen Sie UTF-8 serverübergreifend fest, indem Sie die folgende Option in `my.cnf` (Linux oder Solaris) oder `my.ini` (Windows) aufnehmen:

```
character_set_server=utf8
```

Sie können auch den Zeichensatz für eine Datenbank bei ihrer Erstellung angeben, indem Sie den folgenden Befehl eingeben:

```
create database databasename character set utf8 collate utf8_bin;
```

Wenn Sie den Zeichensatz für die Datenbank festlegen, müssen Sie ihn auch in der JDBC-URL in der Datei `IDM-ds.xml` festlegen. Beispiel:

```
<connection-url>jdbc:mysql://localhost:3306/
databasename?useUnicode=true&amp;characterEncoding=utf8&amp;connectionCollati
on=utf8_bin</connection-url>
```

Beachtung der Groß- und Kleinschreibung

Stellen Sie sicher, dass die Beachtung der Groß- und Kleinschreibung server- bzw. plattformübergreifend einheitlich geregelt ist, falls Daten server- bzw. plattformübergreifend gesichert und wiederhergestellt werden. Sie können die Einheitlichkeit gewährleisten, indem Sie für `lower_case_table_names` in allen `my.cnf`-Dateien (Linux oder Solaris) oder `my.ini`-Dateien (Windows) denselben Wert angeben (0 oder 1), anstatt den vorgegebenen Wert zu übernehmen (die Windows-Vorgabe ist 0, die Linux-Vorgabe ist 1). Legen Sie diesen Wert fest, bevor Sie die Datenbank für die Identity Manager-Tabellen erstellen. Beispiel: Sie definieren

```
lower_case_table_names=1
```

in den `my.cnf`- und `my.ini`-Dateien für alle Plattformen, auf denen eine Datenbank gesichert und wiederhergestellt werden soll.

ANSI-Einstellung

Sie müssen den Eintrag `ansi` zur Datei „my.cnf“ (auf Linux) oder zur Datei „my.ini“ (auf Windows) hinzufügen. Wenn Sie diesen Eintrag nicht hinzufügen, werden die RBPM-Tabellen erstellt, aber die anfänglichen Daten werden nicht geladen und möglicherweise wird die Fehlermeldung „Definition der Gast-Containerseite wurde nicht gefunden“ angezeigt.

Die Datei „my.cnf“ (bzw. „my.ini“) sollte folgendermaßen aussehen, nachdem Sie den `ansi`-Eintrag hinzugefügt haben:

```
# These variables are required for IDM User Application
character_set_server=utf8
default-table-type=innodb

# Put the server in ANSI SQL mode.
#See http://www.mysql.com/doc/en/ANSI_mode.html
ansi
```

Führen Sie zum Bestätigen, dass die Änderung auf Verwendung des ANSI-Modus wirksam wurde, die folgenden SQL-Anweisungen auf dem MySQL-Server aus:

```
mysql> select @@global.sql_mode;
+-------------------------------------------------------------+
| @@global.sql_mode                                           |
+-------------------------------------------------------------+
| REAL_AS_FLOAT,PIPES_AS_CONCAT,ANSI_QUOTES,IGNORE_SPACE,ANSI |
+-------------------------------------------------------------+
1 row in set (0.00 sec)
```

Benutzerkontoanforderungen

Das während der Installation verwendete Benutzerkonto muss Besitzer der Datenbank sein, die von der Benutzeranwendung verwendet wird. Zudem benötigt dieses Benutzerkonto Zugriff auf die Tabellen im System. Je nach Umgebung können die Tabellen unterschiedlich sein.

Erstellen Sie einen Benutzer zur Anmeldung beim MySQL-Server und gewähren Sie ihm Rechte. Beispiel:

```
GRANT ALL PRIVILEGES ON <dbname.>* TO <Benutzername>@ <host> IDENTIFIED BY '
Passwort'
```

Die mindestens erforderlichen Rechte sind: CREATE, INDEX, INSERT, UPDATE, DELETE und LOCK TABLES. Die Dokumentation zum GRANT-Befehl finden Sie unter http://www.mysql.org/doc/refman/5.0/en/grant.html (http://www.mysql.org/doc/refman/5.0/en/grant.html).

Wichtig: Das Benutzerkonto muss auch über „select“-Rechte für die mysql-Benutzertabelle verfügen. Die SQL-Syntax zum Gewähren der geeigneten Rechte:

```
USE mysql;
GRANT SELECT ON mysql.user TO <username>@<host>;
```

2.4.2 Hinweise zum Konfigurieren einer Oracle-Datenbank

Stellen Sie beim Erstellen einer Oracle-Datenbank sicher, dass Sie „AL32UTF8“ zum Angeben eines Unicode-kodierten Zeichensatzes verwenden. (Siehe AL32UTF8 (http://download-east.oracle.com/docs/cd/B19306_01/server.102/b14225/glossary.htm#sthref2039) .)

Sie müssen beim Erstellen eines Benutzers für die Oracle-Datenbank die folgenden Anweisungen mithilfe des SQL Plus-Dienstprogramms ausführen. Diese Befehle erstellen den Benutzer und legen die Rechte des Benutzers fest. Erteilen Sie dem Benutzer CONNECT- und RESOURCE-Rechte, z. B.:

```
CREATE USER idm-Benutzer IDENTIFIED BY Passwort
```

```
GRANT CONNECT, RESOURCE to IDM-Benutzer
```

UTF-8 unter Oracle 11g Sie können unter Oracle 11g den folgenden Befehl ausführen, um zu bestätigen, dass UTF-8 aktiviert ist:

```
select * from nls_database_parameters;
```

Falls UTF-8 nicht eingerichtet ist, werden folgende Daten zurückgegeben:

```
NLS_CHARACTERSET
WE8MSWIN1252
```

Wenn UTF-8 eingerichtet ist, werden folgende Daten zurückgegeben:

```
NLS_CHARACTERSET
AL32UTF8
```

2.4.3 Hinweise zum Konfigurieren einer MS SQL Server-Datenbank

Richten Sie die MS SQL Server-Datenbank wie folgt ein:

1. Installieren Sie den MS SQL-Server.
2. Stellen Sie eine Verbindung zum Server her und öffnen Sie eine Anwendung zur Erstellung der Datenbank und des Datenbankbenutzers (üblicherweise die Anwendung „SQL Server Management Studio“).
3. Erstellen Sie eine Datenbank. SQL Server erlaubt es Benutzern nicht, den Zeichensatz für Datenbanken auszuwählen. Die IDM-Benutzeranwendung speichert SQL Server-Zeichendaten in einem NCHAR-Spaltentyp, der UTF-8 unterstützt.
4. Erstellen Sie eine Anmeldung.
5. Fügen Sie die Anmeldeinformationen für einen Benutzer der Datenbank hinzu.
6. Erteilen Sie der Anmeldung die folgenden Rechte: CREATE TABLE, CREATE INDEX, SELECT, INSERT, UPDATE und DELETE.

Die Benutzeranwendung benötigt Version 1.0.809.102 des JDBC-Treibers für Microsoft SQL Server 2005. Beachten Sie, dass nur die Betriebssysteme Sun Solaris, Red Hat Linux und Windows 2000 oder höher mit diesem JDBC-Treiber offiziell unterstützt werden.

2.4.4 Hinweise zum Konfigurieren einer DB2-Datenbank

In diesem Abschnitt finden Sie Hinweise zum Konfigurieren von DB2.

Bereitstellen der Datenbanktreiber-JAR-Dateien

Die Datenbanktreiber-JAR-Dateien müssen während der Installation auf dem Bildschirm *Datenbankbenutzername und Passwort* ausgewählt werden. Allerdings können Sie mithilfe der Schaltfläche „Durchsuchen“ des Felds *Datenbanktreiber-JAR-Datei* nur eine (1) JAR-Datei auswählen. Sie müssen für DB2 zwei (2) JAR-Dateien angeben:

- db2jcc.jar
- db2jcc_license_cu.jar

Wenn Sie also das Installationsprogramm mit WebSphere (dem einzigen Anwendungsserver, der für DB2 unterstützt wird) ausführen, können Sie nur eine JAR-Datei auswählen. Daher müssen Sie die zweite Datei manuell eingeben und dabei das richtige Dateitrennzeichen für das Betriebssystem verwenden, auf dem das Installationsprogramm ausgeführt wird. Alternativ können Sie beide Dateinamen manuell eingeben.

Zum Beispiel unter Windows:

```
c:\db2jars\db2jcc.jar;c:\db2jars\db2jcc_license_cu.jar
```

Beispielsweise unter Solaris und Linux:

```
/home/lab/db2jars/db2jcc.jar:/home/lab/db2jcc_license_cu.jar
```

DB2-Datenbanken optimieren, um Deadlocks und Zeitüberschreitungen zu verhindern

Wenn Sie bei der Verwendung von DB2 eine Fehlermeldung erhalten, die besagt, dass aufgrund eines Deadlocks oder einer Zeitüberschreitung die aktuelle Transaktion rückabgewickelt wurde, kann dies auf eine hohe gleichzeitige Datenbanknutzung zurückzuführen sein.

DB2 stellt viele Techniken zum Auflösen von Sperrkonflikten bereit, darunter das Optimieren des kostenbasierten Optimierungsprogramms. Das *Leistungshandbuch*, das Bestandteil der DB2-Administratordokumentation ist, ist eine hervorragende Quelle mit vielen Optimierungstipps.

Es gibt keine vorgeschriebenen Optimierungswerte, die für alle Installationen verwendet werden können, da sich das Ausmaß des gemeinsamen Zugriffs und der Umfang der Daten unterscheiden können. Nichtsdestotrotz finden Sie hier einige DB2-Optimierungstipps, die für Ihre Installation von Belang sein könnten:

- Der Befehl `reorgchk update statistics` aktualisiert die vom Optimierungsprogramm verwendeten Statistiken. Allein das regelmäßige Aktualisieren dieser Statistiken könnte genügen, um das Problem zu beheben.
- Durch die Verwendung des DB2-Registrierungsparameters DB2_RR_TO_RS könnte der gemeinsame Zugriff verbessert werden, indem der nächste Schlüssel der Zeile, die eingefügt oder aktualisiert wurde, nicht gesperrt wird.
- Erhöhen Sie die Werte für MAXLOCKS und LOCKLIST für die Datenbank.
- Erhöhen Sie den Wert der currentLockTimeout-Eigenschaft für den Datenbank-Verbindungspool.
- Verwenden Sie den Database Configuration Advisor und optimieren Sie für schnellere Transaktionen.
- Ändern Sie alle Tabellen der Benutzeranwendung auf VOLATILE, damit das Optimierungsprogramm weiß, dass die Kardinalität der Tabelle deutlich abweichen kann. Beispielsweise können Sie die AFACTIVITY-Tabelle VOLATILE machen, indem Sie folgenden Befehl ausführen: `ALTER TABLE AFACTIVITY VOLATILE`

Die ALTER TABLE-Befehle müssen ausgeführt werden, nachdem die Benutzeranwendung einmal gestartet wurde und die Datenbanktabellen erstellt wurden. Weitere Informationen zu dieser Anweisung finden Sie in der Dokumentation zu ALTER TABLE. Nachfolgend stehen die SQL-Anweisungen für alle Benutzeranwendungstabellen:

```
ALTER TABLE AFACTIVITY VOLATILE
ALTER TABLE AFACTIVITYTIMERTASKS VOLATILE
ALTER TABLE AFBRANCH VOLATILE
ALTER TABLE AFCOMMENT VOLATILE
ALTER TABLE AFDOCUMENT VOLATILE
ALTER TABLE AFENGINE VOLATILE
ALTER TABLE AFENGINESTATE VOLATILE
ALTER TABLE AFMODEL VOLATILE
ALTER TABLE AFPROCESS VOLATILE
ALTER TABLE AFPROVISIONINGSTATUS VOLATILE
ALTER TABLE AFQUORUM VOLATILE
ALTER TABLE AFRESOURCEREQUESTINFO VOLATILE
ALTER TABLE AFWORKTASK VOLATILE
ALTER TABLE AF_ROLE_REQUEST_STATUS VOLATILE
ALTER TABLE ATTESTATION_ATTESTER VOLATILE
ALTER TABLE ATTESTATION_ATTRIBUTE VOLATILE
ALTER TABLE ATTESTATION_QUESTION VOLATILE
ALTER TABLE ATTESTATION_REPORT VOLATILE
ALTER TABLE ATTESTATION_REQUEST VOLATILE
ALTER TABLE ATTESTATION_RESPONSE VOLATILE
ALTER TABLE ATTESTATION_SURVEY_QUESTION VOLATILE
ALTER TABLE ATTESTATION_TARGET VOLATILE
ALTER TABLE AUTHPROPS VOLATILE
ALTER TABLE DATABASECHANGELOG VOLATILE
ALTER TABLE DATABASECHANGELOGLOCK VOLATILE
ALTER TABLE DSS_APPLET_BROWSER_TYPES VOLATILE
ALTER TABLE DSS_APPLET_CFG VOLATILE
ALTER TABLE DSS_APPLET_CFG_MAP VOLATILE
ALTER TABLE DSS_BROWSER_TYPE VOLATILE
ALTER TABLE DSS_CONFIG VOLATILE
ALTER TABLE DSS_EXT_KEY_USAGE_RESTRICTION VOLATILE
ALTER TABLE DSS_USR_POLICY_SET VOLATILE
ALTER TABLE JBM_COUNTER VOLATILE
ALTER TABLE JBM_DUAL VOLATILE
ALTER TABLE JBM_ID_CACHE VOLATILE
ALTER TABLE JBM_MSG VOLATILE
ALTER TABLE JBM_MSG_REF VOLATILE
ALTER TABLE JBM_POSTOFFICE VOLATILE
ALTER TABLE JBM_ROLE VOLATILE
ALTER TABLE JBM_TX VOLATILE
ALTER TABLE JBM_USER VOLATILE
ALTER TABLE PORTALCATEGORY VOLATILE
ALTER TABLE PORTALPORTLETHANDLES VOLATILE
ALTER TABLE PORTALPORTLETSETTINGS VOLATILE
ALTER TABLE PORTALPRODUCERREGISTRY VOLATILE
ALTER TABLE PORTALPRODUCERS VOLATILE
ALTER TABLE PORTALREGISTRY VOLATILE
ALTER TABLE PROFILEGROUPPREFERENCES VOLATILE
ALTER TABLE PROFILEUSERPREFERENCES VOLATILE
ALTER TABLE PROVISIONING_CODE_MAP VOLATILE
ALTER TABLE PROVISIONING_CODE_MAP_LABEL VOLATILE
ALTER TABLE PROVISIONING_VIEW_VALUE VOLATILE
```

```
ALTER TABLE PROVISIONING_VIEW_VALUE_LABEL VOLATILE
ALTER TABLE SECURITYACCESSRIGHTS VOLATILE
ALTER TABLE SECURITYPERMISSIONMETA VOLATILE
ALTER TABLE SECURITYPERMISSIONS VOLATILE
ALTER TABLE SEC_DELPROXY_CFG VOLATILE
ALTER TABLE SEC_DELPROXY_SRV_CFG VOLATILE
ALTER TABLE SEC_SYNC_CLEANUP_QUEUE VOLATILE
```

2.5 Installieren des Java Development Kit

Das Installationsprogramm für die Benutzeranwendung setzt voraus, dass Sie die richtige Version der Java-Umgebung für Ihren Anwendungsserver verwenden, wie unten beschrieben:

- Sie müssen für JBoss 5.01 die Java 2 Platform Standard Edition Development Version 1.6 (JDK oder JRE) von Sun verwenden.

  Hinweis: Das benutzerfreundliche JBossPostgreSQL-Dienstprogramm installiert die korrekte Version von JRE für JBoss.

- Sie müssen für WebSphere 7.0 das JDK 1.6 von IBM verwenden.
- Sie müssen für WebLogic 10.3 das JDK 1.6 von JRockit verwenden.

Setzen Sie die Umgebungsvariable JAVA_HOME so, dass sie auf das JDK verweist, das mit der Benutzeranwendung verwendet werden soll. Alternativ können Sie den Pfad während der Installation der Benutzeranwendung manuell eingeben, um JAVA_HOME zu überschreiben.

Hinweis: Für Benutzer von SUSE Linux Enterprise Server (SLES): Verwenden Sie nicht das mit SLES mitgelieferte IBM JDK. Diese Version ist mit einigen Aspekten der Installation nicht kompatibel.

Installation des rollenbasierten Bereitstellungsmoduls

3

In diesem Abschnitt wird beschrieben, wie die Laufzeitkomponenten für das rollenbasierte Bereitstellungsmodul (RBPM) in Identity Manager unter Verwendung des Installationsprogramms für das rollenbasierte Bereitstellungsmodul installiert werden. Es werden u. a. folgende Themen erläutert:

- Abschnitt 3.1, „Installieren des rollenbasierten Bereitstellungsmoduls“, auf Seite 33
- Abschnitt 3.2, „Ausführen des Dienstprogramms „NrfCaseUpdate““, auf Seite 34
- Abschnitt 3.3, „Ausführen des RBPM-Installationsprogramms“, auf Seite 40
- Abschnitt 3.4, „Schema manuell erweitern“, auf Seite 47

Wichtig: In dieser Version können Sie den Benutzeranwendungstreiber sowie den Rollen- und Ressourcenservice-Treiber nicht mehr über iManager erstellen. Diese Methode des Erstellens von Treibern wird nicht mehr unterstützt. Zum Erstellen dieser Treiber müssen Sie die neuen Paketverwaltungsfunktionen von Designer verwenden, wie in Kapitel 4, „Erstellen der Treiber“, auf Seite 49 beschrieben.

3.1 Installieren des rollenbasierten Bereitstellungsmoduls

Identity Manager 4.0 installiert automatisch die wichtigsten Laufzeitkomponenten des RBPM. Allerdings können Sie das Installationsprogramm für das rollenbasierte Bereitstellungsmodul auch separat aufrufen.

Das RBPM-Installationsprogramm muss auf dem Computer ausgeführt werden, auf dem die Identity Manager-Metaverzeichnisumgebung installiert wurde. Die Installation schlägt fehl, wenn eDirectory nicht am Standardspeicherort oder am Standard-dib-Speicherort installiert ist.

Hinweis: Das RBPM-Installationsprogramm kann auch dann nicht ordnungsgemäß ausgeführt werden, wenn eDirectory nicht auf den Standard-LDAP-Ports 389 und 636 ausgeführt wird. Wenn keine Ausführung auf den Standard-LDAP-Ports erfolgt, erhalten Sie ständig die Meldung, dass das Schema nicht gültig ist und dass Sie das NrfCaseUpdate-Dienstprogramm ausführen müssen. Sie müssen zum Beheben dieses Problems das Schema manuell erweitern, wie in Abschnitt 3.4, „Schema manuell erweitern“, auf Seite 47 beschrieben.

Nachdem diese Elemente in Identity Manager installiert wurden, müssen Sie die unter Kapitel 4, „Erstellen der Treiber“, auf Seite 49 beschriebenen Schritte ausführen, um die zum Ausführen der Benutzeranwendung erforderlichen Treiber zu erstellen.

Wichtig: Falls sich ein Benutzeranwendungstreiber, der mit Version 3.6.1 oder einer früheren Version des RBPMs erstellt wurde, in Ihrem eDirectory-Baum befindet, müssen Sie das Dienstprogramm „NrfCaseUpdate“ ausführen, bevor Sie das Installationsprogramm des

rollenbasierten Bereitstellungsmoduls ausführen. Wenn Sie dies nicht tun, schlägt die Installation fehl. Dieser Schritt ist nicht erforderlich, wenn Sie eine Neuinstallation von Version 4.0 oder eine Aufrüstung von Version 3.7 vornehmen.

3.2 Ausführen des Dienstprogramms „NrfCaseUpdate“

In diesem Abschnitt wird das Dienstprogramm „NrfCaseUpdate“ beschrieben. Es werden u. a. folgende Themen erläutert:

- Abschnitt 3.2.1, „Überblick über NrfCaseUpdate“, auf Seite 34
- Abschnitt 3.2.2, „Installationsüberblick“, auf Seite 34
- Abschnitt 3.2.3, „Wie sich „NrfCaseUpdate“ auf das Schema auswirkt“, auf Seite 35
- Abschnitt 3.2.4, „Erstellen einer Sicherungskopie der Benutzeranwendungstreiber“, auf Seite 35
- Abschnitt 3.2.5, „Verwenden von NrfCaseUpdate“, auf Seite 35
- Abschnitt 3.2.6, „Verifizierung des „NrfCaseUpdate“-Prozesses“, auf Seite 38
- Abschnitt 3.2.7, „Aktivieren der JRE für SSL-Verbindungen“, auf Seite 38
- Abschnitt 3.2.8, „Wiederherstellen ungültig gemachter Benutzeranwendungstreiber“, auf Seite 39

3.2.1 Überblick über NrfCaseUpdate

Die NrfCaseUpdate-Prozedur ist erforderlich, um bei Beachtung der Groß-/Kleinschreibung Suchen nach Rollen und Ressourcen durchzuführen. Diese Prozedur aktualisiert das Schema, indem sie die von den Benutzeranwendungstreibern verwendeten Attribute „nrfLocalizedDescrs“ und „nrfLocalizedNames“ ändert. Das Verfahren ist erforderlich, bevor Sie RBPM 4.0 installieren und bevor Sie vorhandene Treiber in Designer 4.0 migrieren, wenn Ihr eDirectory-Baum mit Version 3.6.1 oder einer früheren Version des RBPMs erstellt wurde. Dieser Schritt ist nicht erforderlich, wenn Sie eine Neuinstallation von Version 4.0 oder eine Aufrüstung von Version 3.7 vornehmen.

3.2.2 Installationsüberblick

Dieser Abschnitt bietet einen Überblick über die Schritte zum Aufrüsten und Migrieren einer vorhandenen RBPM-Umgebung. Dieser Überblick unterstreicht die Verwendung von Designer 4.0 zum Erstellen von Sicherungskopien der Benutzeranwendungstreiber vor dem Aufrüsten. In diesem Überblick wird auch davon ausgegangen, dass die IDM-Version 3.6 oder höher ist.

1. Installieren Sie Designer 4.0.
2. Führen Sie eine Zustandsüberprüfung des Identitätsdepots aus, um sicherzustellen, dass das Schema ordnungsgemäß erweitert wird. Verwenden Sie TID 3564075 zum Durchführen der Zustandsüberprüfung.
3. Importieren Sie vorhandene Benutzeranwendungstreiber nach Designer 4.0.
4. Archivieren Sie das Designer-Projekt. Es stellt den Zustand des Treibers vor RBPM 4.0 dar.
5. Führen Sie den NrfCaseUpdate-Prozess aus.

6. Erstellen Sie ein neues Designer 4.0-Projekt und importieren Sie den Benutzeranwendungstreiber, um die Migration vorzubereiten.
7. Installieren Sie RBPM 4.0.
8. Migrieren Sie den Treiber mithilfe von Designer 4.0.
9. Stellen Sie den migrierten Treiber bereit.

3.2.3 Wie sich „NrfCaseUpdate“ auf das Schema auswirkt

Wenn das Dienstprogramm „NrfCaseUpdate“ vorhandene Attribute im eDirectory-Schema aktualisiert, werden alle vorhandenen Instanzen dieser Attribute effektiv gelöscht. Benutzeranwendungstreiber verwenden diese Attribute und werden daher von dieser Schema-Aktualisierung betroffen, darunter Namen und Beschreibungen von Rollen und Funktionstrennungen, benutzerdefinierte Beglaubigungsanforderungen and Berichte.

Die NrfCaseUpdate-Prozedur aktualisiert vorhandene Benutzeranwendungstreiber, indem sie ein Dienstprogramm bereitstellt, das vorhandene Benutzeranwendungstreiber in eine LDIF-Datei exportiert, bevor das Schema aktualisiert wird. Durch das Importieren der LDIF-Dateien nach dem Aktualisieren des Schemas können die während des Aktualisierens des Schemas gelöschten Objekte effektiv wiederhergestellt werden.

Es ist wie immer wichtig, dass Sie vorsichtshalber alle vorhandenen Benutzeranwendungstreiber sichern. Denken Sie daran, dass sich Schema-Aktualisierungen auf alle IDM-Partitionen auswirken. Deshalb ist es wichtig, dass Sie „NrfCaseUpdate“ verwenden, um alle Benutzeranwendungstreiber im Baum zu exportieren.

3.2.4 Erstellen einer Sicherungskopie der Benutzeranwendungstreiber

Es wird empfohlen, dass Sie Designer zum Erstellen einer Sicherungskopie Ihrer Benutzeranwendungstreiber verwenden. Sie sollten diese Prozedur zum Sichern Ihrer vorhandenen Benutzeranwendungstreiber durchführen, bevor Sie die NrfCaseUpdate-Prozedur durchführen:

1. Installieren Sie Designer 4.0 (in RBPM 4.0 enthalten).
2. Erstellen Sie ein Identitätsdepot und ordnen Sie es dem IDM-Server mit Ihren Benutzeranwendungstreibern zu.
3. Verwenden Sie zum Importieren Ihres Treibersatzes und der Benutzeranwendungstreiber den Befehl *Live->Importieren*.
4. Speichern und archivieren Sie dieses Designer-Projekt.

3.2.5 Verwenden von NrfCaseUpdate

NrfCaseUpdate fordert Sie auf, alle Treiber zu exportieren, und führt anschließend das Aktualisieren des Schemas aus. Fahren Sie nicht fort, wenn Sie nicht sicher sind, ob Benutzeranwendungstreiber vorhanden sind bzw. wo vorhandene Treiber sich befinden, da die Schema-Aktualisierung möglicherweise alle vorhandenen Benutzeranwendungstreiber ungültig macht.

Die JRE, die sich unter dem IDM-Installationsverzeichnis befindet (in der Regel `/root/idm/jre`), kann zum Ausführen von „NrfCaseUpdate“ verwendet werden. Falls Sie SSL-Verbindungen mit eDirectory benötigen, müssen Sie Ihre JRE für SSL-Verbindungen aktivieren. Befolgen Sie hierzu die Anweisungen unter Abschnitt 3.2.7, „Aktivieren der JRE für SSL-Verbindungen“, auf Seite 38.

Alternativ können Sie das Dienstprogramm „NrfCaseUpdate“ remote von einem Host mit einer JRE ausführen, der das eDirectory-Zertifikat enthält, z. B. dem Benutzeranwendungs-Server. In diesem Fall müssen Sie nach dem Exportieren aller Treiber in die LDIF-Datei und vor dem Aktualisieren des Schemas das Dienstprogramm „NrfCaseUpdate“ mit STRG+C beenden. Anschließend können Sie das Schema auf dem eDirectory-Host manuell mit dem Befehl „ndssch“ aktualisieren, wie unten dargestellt:

```
ndssch -h hostname adminDN update-nrf-case.sch
```

Hinweis: Bei „NrfCaseUpdate“ können mehrere Argumente in der Befehlszeile angegeben werden. Geben Sie für weitere Informationen `-help` oder `-? an`.

Führen Sie folgende Schritte aus, um „NrfCaseUpdate“ auszuführen:

1. Stellen Sie sicher, dass eine Zustandsüberprüfung des Identitätsdepots durchgeführt wurde, bevor Sie das NrfCaseUpdate-Dienstprogramm ausführen. Verwenden Sie TID 3564075 zum Durchführen der Zustandsüberprüfung.
2. Identifizieren Sie alle DNs der vorhandenen Benutzeranwendungstreiber, bevor Sie das Dienstprogramm starten. Sie benötigen einen Berechtigungsnachweis zum Authentifizieren, um diese Treiber in eine LDIF-Datei zu exportieren.
3. Führen Sie das Dienstprogramm „NrfCaseUpdate“ aus. Sie können auch die Option `-v` angeben, um eine ausführlichere Ausgabe zu erhalten:

   ```
   /root/idm/jre/bin/java -jar NrfCaseUpdate.jar -v
   ```
4. Sie werden gefragt, ob Sie einen vorhandenen Benutzeranwendungstreiber haben. Beantworten Sie die Frage mit „Wahr“, wenn Sie einen vorhandenen Benutzeranwendungstreiber haben. Anderenfalls beantworten Sie mit „Falsch“ und fahren Sie mit Schritt 6 auf Seite 36 fort.

   ```
   Do you currently have a User Application Driver configured [DEFAULT true]
   :
   ```
5. Als Nächstes werden Sie gefragt, ob Sie mehrere Benutzeranwendungstreiber haben. Beantworten Sie die Frage mit „Wahr“, wenn Sie mehrere Benutzeranwendungstreiber haben:

   ```
   Do you currently have more than one (1) User Application Driver configured
   [DEFAULT false] :
   ```
6. Geben Sie den DN des Administrators mit dem Berechtigungsnachweis zum Exportieren des Benutzeranwendungstreibers an:

   ```
   Specify the DN of the Identity Vault administrator user.
   This user must have inherited supervisor rights to the user application
   driver specified above.
   (e.g. cn=admin,o=acme):
   ```
7. Geben Sie das Passwort für diesen Administrator an:

   ```
   Specify the Identity Vault administrator password:
   ```
8. Geben Sie den Hostnamen oder die IP-Adresse des IDM-Servers an, auf dem sich der Benutzeranwendungstreiber befindet:

   ```
   Specify the DNS address of the Identity Vault (e.g acme.com):
   ```
9. Geben Sie den Port für die Verbindung an:

```
Specify the Identity Vault port [DEFAULT 389]:
```

10 Als Nächstes werden Sie gefragt, ob Sie für die Verbindung SSL verwenden werden. Wenn Sie SSL verwenden möchten, setzt die JRE voraus, dass sich das eDirectory-Zertifikat im Herkunftsverbürgungs-Keystore befindet. Befolgen Sie zum Aufbewahren des Zertifikats die Anweisungen in Abschnitt 3.2.7, „Aktivieren der JRE für SSL-Verbindungen“, auf Seite 38.

```
Use SSL to connect to Identity Vault: [DEFAULT false] :
```

11 Geben Sie den vollständig qualifizierten, eindeutigen Namen des zu exportierenden Benutzeranwendungstreibers an:

```
Specify the fully qualified LDAP DN of the User Application driver located
in the Identity Vault
(e.g. cn=UserApplication,cn=driverset,o=acme):
```

Falls der DN ein Leerzeichen enthalt, muss es in einfache Anführungszeichen gesetzt werden, wie nachfolgend dargestellt:

```
'cn=UserApplication driver,cn=driverset,o=acme'
```

12 Geben Sie einen Namen für die LDIF-Datei an, in die die Benutzeranwendung exportiert wird:

```
Specify the LDIF file name where the restore data will be written (enter
defaults to nrf-case-restore-data.ldif):
```

13 Das Dienstprogramm veröffentlicht Informationen über die in der LDIF-Datei gespeicherten Objekte.

14 Wenn Sie angegeben haben, dass Sie über mehrere Treiber verfügen, erscheint die folgende Aufforderung:

```
You indicated you have more than one (1) User Application Driver to
configure.
Do you have another driver to export? [DEFAULT false] :

If you have another driver to export then specify true. The utility will
repeat Steps 5 through 12 for each driver.

If you do not have another driver to export then specify false. Ensure that
you have exported all existing drivers before proceeding as the utility
will proceed with the schema update.
```

15 Sie werden aufgefordert, den Speicherort des Dienstprogramms `ndssch` anzugeben. Das Dienstprogramm `ndssch` wird zum Aktualisieren des Schemas verwendet.

```
Please enter the path to the schema utility:
For Unix/Linux typically /opt/novell/eDirectory/bin/ndssch
For Windows C:\Novell\NDS\schemaStart.bat:
```

16 Das Dienstprogramm veröffentlicht die Statusmeldung für die Schema-Aktualisierung:

```
Schema has successfully been updated for mixed case compliance!
```

Hinweis: Lassen Sie eDirectory genügend Zeit für die Synchronisierung der Schemaänderungen. Wenn Sie nicht genügend Zeit gewähren, schlägt der Import der LDIF-Datei fehl.

---

17 Führen Sie eine weitere Zustandsüberprüfung des Identitätsdepots durch, um sicherzustellen, dass das Schema vor dem Import der LDIF-Datei ordnungsgemäß importiert wurde. Verwenden Sie TID 3564075 zum Durchführen der Zustandsüberprüfung.

18 Nachdem alle Treiber exportiert wurden und die Schema-Aktualisierung erfolgreich angewendet wurde, müssen Sie die LDIF-Dateien importieren. Sie sollten beim Ausführen des Befehls `ice` angeben, dass Vorverweise erlaubt werden sollen. Nachfolgend finden Sie einen Vorschlag für die Befehlszeile:

```
ice -l [mylogfile.log] -v -SLDIF -f [your_created_ldif] -c -DLDAP -s
[hostname] -p [389/636] -d [cn=myadmin,o=mycompany] -w [MYPASSWORD] -F -B
```

19 Vergewissern Sie sich, nachdem alle Treiber erneut importiert wurden, dass der „NrfCaseUpdate“-Prozess erfolgreich abgeschlossen wurde. Weitere Informationen finden Sie unter Abschnitt 3.2.6, „Verifizierung des „NrfCaseUpdate“-Prozesses“, auf Seite 38.

20 Nachdem Sie sich vergewissert haben, dass der „NrfCaseUpdate“-Prozess erfolgreich abgeschlossen wurde, können Sie mit der Installation von RBPM 4.0 fortfahren.

3.2.6 Verifizierung des „NrfCaseUpdate“-Prozesses

Vergewissern Sie sich, nachdem alle Treiber erneut importiert wurden, dass die Wiederherstellung erfolgreich verlaufen ist, indem Sie die folgenden Begriffe in der Benutzeranwendung überprüfen:

- Rollennamen und -beschreibungen
- Funktionstrennungsnamen und -beschreibungen
- Beglaubigungsanforderungen einschließlich benutzerdefinierter Anforderungen
- Berichte

Nach Abschluss der Verifizierung können Sie mit der Installation und Aufrüstung auf RBPM 4.0 fortfahren.

3.2.7 Aktivieren der JRE für SSL-Verbindungen

In diesem Abschnitt wird beschrieben, wie die JRE zum Verwenden einer SSL-Verbindung konfiguriert wird.

Exportieren Sie zunächst ein eigensigniertes Zertifikat aus der Zertifizierungsstelle im Identitätsdepot:

1 Klicken Sie in der Ansicht *Rollen und Aufgaben* des iManagers auf *Verzeichnisadministration* > *Objekt ändern*.

2 Wählen Sie das Zertifizierungsstellenobjekt für das Identitätsdepot aus und klicken Sie auf *OK*. Gewöhnlich befindet es sich im Sicherheitscontainer unter dem Namen *TREENAME* CA.Security.

3 Klicken Sie auf *Zertifikat* > *Eigensigniertes Zertifikat*.

4 Klicken Sie auf *Exportieren*.

5 Wenn Sie gefragt werden, ob der private Schlüssel mit dem Zertifikat exportiert werden soll, klicken Sie auf *Nein* und klicken Sie anschließend auf *Weiter*.

6 Wählen Sie das binäre DER-Format.

7 Klicken Sie auf den Link *Exportiertes Zertifikat speichern*.

8 Navigieren Sie zu dem Speicherort auf Ihrem Computer, in dem Sie die Datei speichern möchten, und klicken Sie anschließend auf *Speichern*.

9 Klicken Sie auf *Schließen*.

Importieren Sie dann das eigensigniertes Zertifikat in den Herkunftsverbürgungs-Keystore der JRE.

1. Verwenden Sie das Keytool-Dienstprogramm der JRE.
2. Importieren Sie das Zertifikat in den Verbürgungsspeicher des Rollenzuordnungsadministrators, indem Sie in der Befehlszeile den folgenden Befehl eingeben:

   ```
   keytool -import -file name_of_cert_file -trustcacerts -noprompt -keystore filename -storepass password
   ```

   Beispiel:

   ```
   keytool -import -file tree_ca_root.b64 -trustcacerts -noprompt -keystore cacerts -storepass changeit
   ```

3.2.8 Wiederherstellen ungültig gemachter Benutzeranwendungstreiber

Wenn eine Schema-Aktualisierung auf einen vorhandenen Benutzeranwendungstreiber angewendet wird, bevor der Treiber mithilfe von „NrfCaseUpdate“ verarbeitet wurde, wird er ungültig gemacht. Sie müssen den Treiber dann mithilfe einer Datensicherung wiederherstellen.

Wichtig: Es ist unerlässlich, dass Sie den ungültig gemachten Benutzeranwendungstreiber *nicht* löschen oder umbenennen, da sonst alle Verknüpfungen des Treibers auch ungültig werden. Wenn zudem der Rollen- und Ressourcenservice-Treiber läuft und Sie den Benutzeranwendungstreiber löschen, erkennt der Rollen- und Ressourcendiensttreiber die Rollenlöschungen und entfernt die Rollen von den jeweiligen Benutzern.

Zudem ist es nicht ausreichend, den gesicherten Treiber neu in IDM bereitzustellen, denn auf diese Weise kann die Schema-Änderung nicht wieder zusammengeführt werden. Anhand der nachfolgenden Prozedur wird die Wiederherstellung durchgeführt, indem eine umbenannte Kopie des Treibers bereitgestellt wird, sodass die wiederherzustellenden Daten generiert werden.

Die folgende Prozedur bietet einen Überblick über den Prozess zum Wiederherstellen des gesicherten Benutzeranwendungstreibers mithilfe von Designer 4.0:

1. Starten Sie den eDirectory-Server neu, um sicher zu gehen, dass die Schema-Änderung wirksam wird.
2. Öffnen Sie eine Kopie des Designer 4.0-Projekts mit der Sicherungskopie des Benutzeranwendungstreibers „UserAppDriver“. Da diese Prozedur den Treibernamen ändert, ist es wichtig, eine Kopie des Projekts zu verwenden.
3. Wählen Sie den Anschluss zwischen dem Benutzeranwendungstreiber und dem Identitätsdepot aus, klicken Sie mit der rechten Maustaste und wählen Sie *Eigenschaften*.
4. Geben Sie einen neuen Namen an, wie z. B. `UserAppDriver_wiederherstellen`. Wählen Sie *Anwenden* und *OK*.
5. Klicken Sie auf *Speichern*, um das Projekt zu speichern.
6. Synchronisieren Sie das Identitätsdepotschema, indem Sie das Identitätsdepot auswählen und *Live->Schema->Vergleichen* wählen und *Designer für die Abgleichsaktion aktualisieren* auswählen.
7. Speichern Sie das Projekt.

8 Stellen Sie den umbenannten Treiber bereit, indem Sie den Treiber auswählen und *Treiber-> Bereitstellen* wählen.

9 Führen Sie „NrfCaseUpdate“ aus und exportieren Sie den neu benannten Treiber in eine LDIF-Datei.

10 Erstellen Sie eine Kopie der LDIF-Datei zum Bearbeiten.

11 Bearbeiten Sie die LDIF-Datei und benennen Sie alle Treiberbezüge um, um den Benutzeranwendungstreiber, den Sie wiederherstellen, widerzuspiegeln. Wenn z. B. Ihr ursprünglicher Benutzeranwendungstreiber `cn=UserAppDriver` ist, würden Sie `cn=UserAppDriver_wiederherstellen` in `cn=UserAppDriver` umbenennen. Dieser Schritt sorgt dafür, dass effektiv eine LDIF-Datei erstellt wird, die den tatsächlichen Benutzeranwendungstreiber widerspiegelt.

12 Verwenden Sie „ice“ zum Importieren der geänderten LDIF-Datei:

```
ice -l[mylogfile.log] -v -SLDIF -f[your_created_ldif] -c -DLDAP -
s[hostname] -p[389/636] -d[cn=myadmin,o=mycompany] -w[MYPASSWORD] -F -B
```

13 Überprüfen Sie mithilfe von „ice“ den Status des Importvorgangs, um sicher zu gehen, dass er erfolgreich war.

14 Befolgen Sie die Anweisungen unter Abschnitt 3.2.6, „Verifizierung des „NrfCaseUpdate“-Prozesses“, auf Seite 38, um die Wiederherstellung des Treibers zu verifizieren.

15 Löschen Sie den umbenannten Treiber aus dem Treibersatz.

3.3 Ausführen des RBPM-Installationsprogramms

1 Starten Sie das Installationsprogramm für Ihre Plattform:

Linux

`rbpm_driver_install_linux.bin`

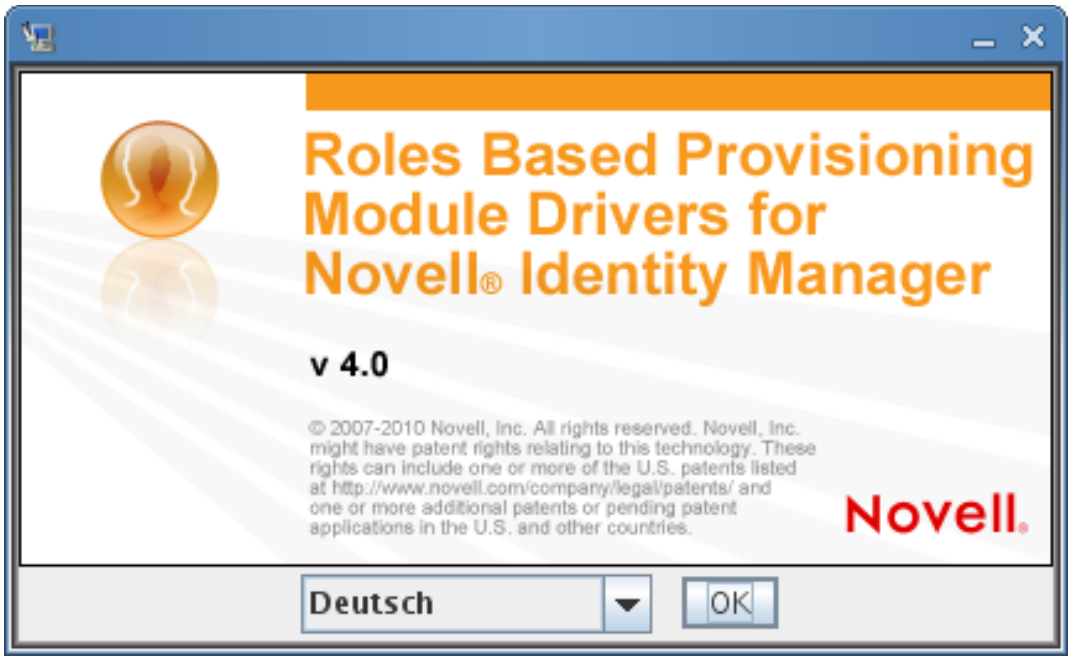
Solaris

`rbpm_driver_install_solaris.bin`

Windows

`rbpm_driver_install.exe`

Wenn das Installationsprogramm startet, werden Sie nach der Sprache gefragt:


Roles Based Provisioning Module Drivers for Novell® Identity Manager
v 4.0
© 2007-2010 Novell, Inc. All rights reserved. Novell, Inc. might have patent rights relating to this technology. These rights can include one or more of the U.S. patents listed at http://www.novell.com/company/legal/patents/ and one or more additional patents or pending patent applications in the U.S. and other countries.
Novell
Deutsch
OK

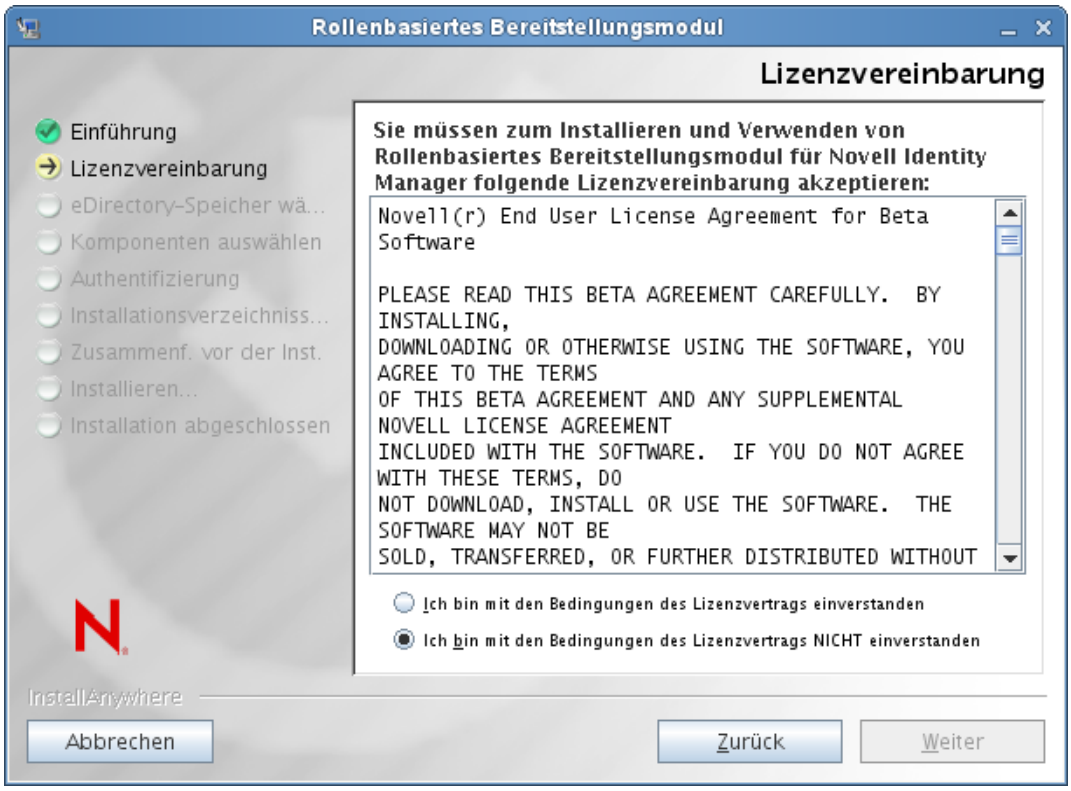
2 Wählen Sie die Sprache für Ihre Installation aus und klicken Sie auf „OK“.

Der Einführungsbildschirm des Installationsprogramms wird angezeigt.

Rollenbasiertes Bereitstellungsmodul
Einführung
Einführung
Lizenzvereinbarung
eDirectory-Speicher wä...
Komponenten auswählen
Authentifizierung
Installationsverzeichniss...
Zusammenf. vor der Inst.
Installieren...
Installation abgeschlossen
Willkommen bei der Installation des Treibers für das rollenbasierte Bereitstellungsmodul für Novell Identity Manager. Dieses Dienstprogramm installiert sowohl den Service-Treiber 'Rollen und Ressourcen' als auch den Benutzeranwendungstreiber. Darüber hinaus wird das Schema erweitert und die Konfigurationsdateien werden installiert. Dies sind die Voraussetzungen für das Installieren des rollenbasierten Bereitstellungsmoduls.
InstallAnywhere
Abbrechen
Zurück
Weiter

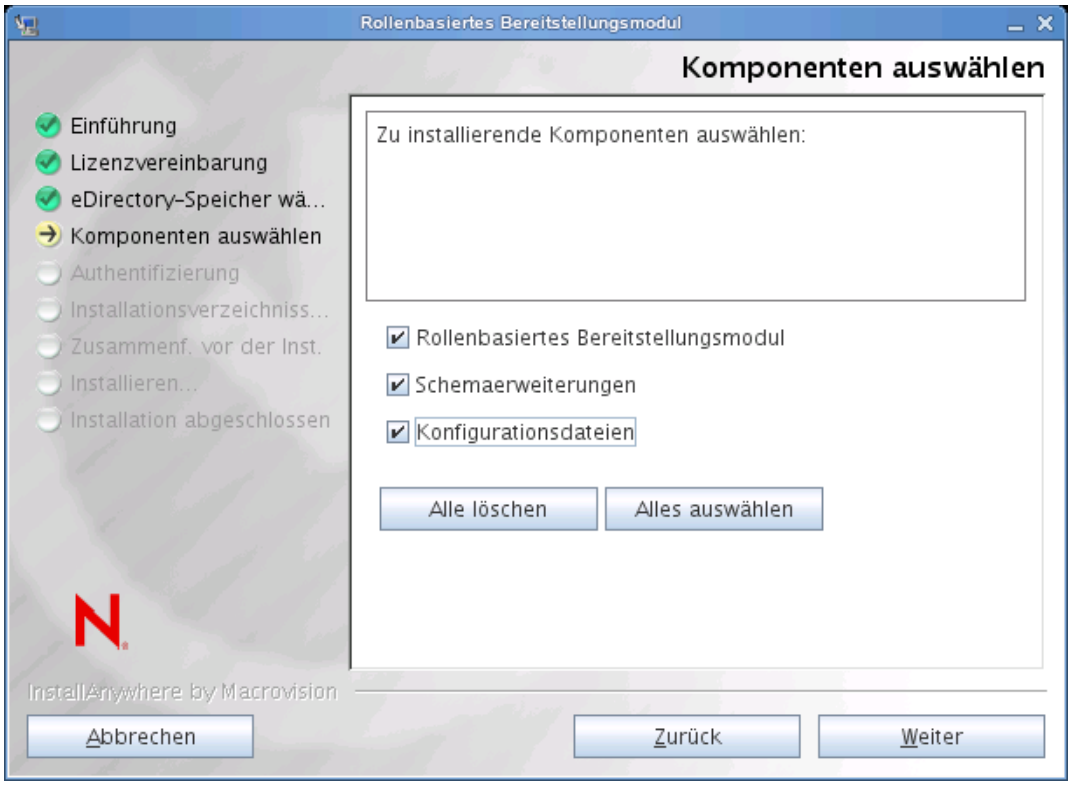
3 Klicken Sie auf *Weiter*.

Der Lizenzvereinbarungsbildschirm des Installationsprogramms wird angezeigt.


Rollenbasiertes Bereitstellungsmodul
Lizenzvereinbarung
Einführung
Lizenzvereinbarung
eDirectory-Speicher wä...
Komponenten auswählen
Authentifizierung
Installationsverzeichniss...
Zusammenf. vor der Inst.
Installieren...
Installation abgeschlossen
Sie müssen zum Installieren und Verwenden von Rollenbasiertes Bereitstellungsmodul für Novell Identity Manager folgende Lizenzvereinbarung akzeptieren:
Novell(r) End User License Agreement for Beta Software
PLEASE READ THIS BETA AGREEMENT CAREFULLY. BY INSTALLING,
DOWNLOADING OR OTHERWISE USING THE SOFTWARE, YOU AGREE TO THE TERMS
OF THIS BETA AGREEMENT AND ANY SUPPLEMENTAL NOVELL LICENSE AGREEMENT
INCLUDED WITH THE SOFTWARE. IF YOU DO NOT AGREE WITH THESE TERMS, DO
NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE. THE SOFTWARE MAY NOT BE
SOLD, TRANSFERRED, OR FURTHER DISTRIBUTED WITHOUT
Ich bin mit den Bedingungen des Lizenzvertrags einverstanden
Ich bin mit den Bedingungen des Lizenzvertrags NICHT einverstanden
InstallAnywhere
Abbrechen
Zurück
Weiter

4 Bestätigen Sie die Lizenzvereinbarung, und klicken Sie auf *Weiter*.

Der Bildschirm „Komponenten auswählen“ des Installationsprogramms, in dem die für das Ausführen der RBPM-Benutzeranwendung erforderlichen Metaverzeichniskomponenten aufgeführt sind, wird angezeigt:

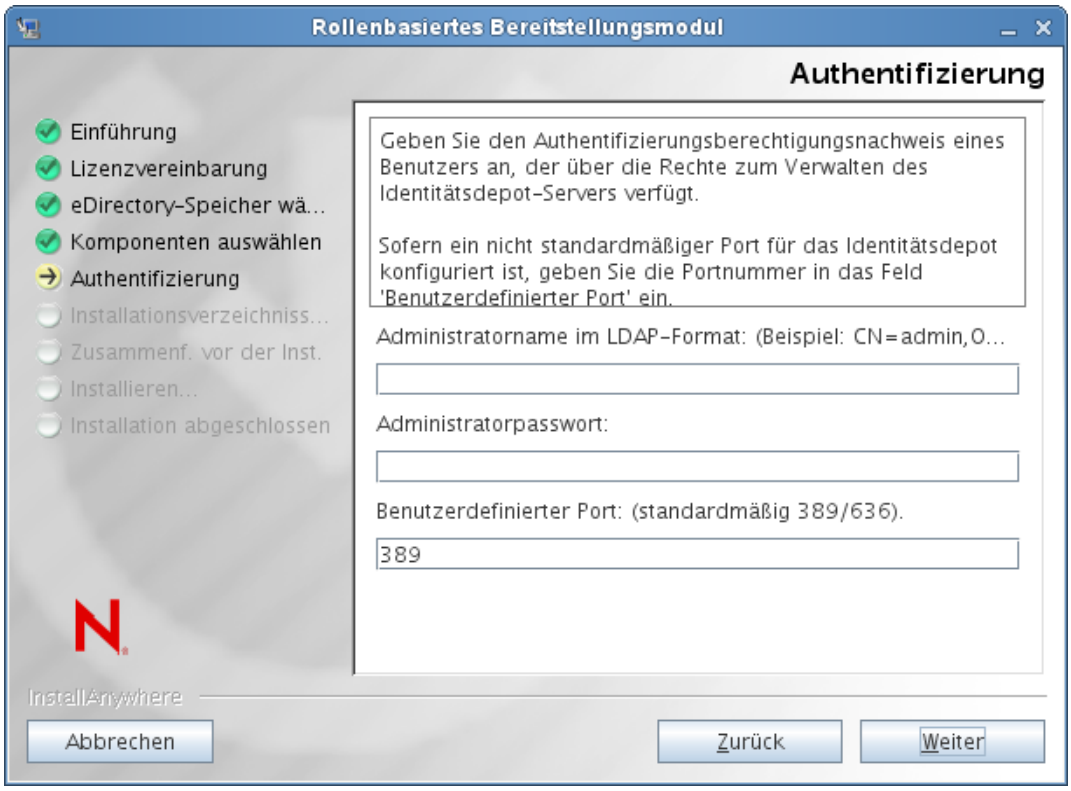


Die Komponenten werden nachfolgend beschrieben:

Komponente	Beschreibung
Rollenbasiertes Bereitstellungsmodul	Installiert den Benutzeranwendungstreiber und den Rollen- und Ressourcentreiber.
Schemaerweiterungen	Installiert die eDirectory-Schemaerweiterungen.
Konfigurationsdateien	Installiert die Treiberkonfigurationsdateien.

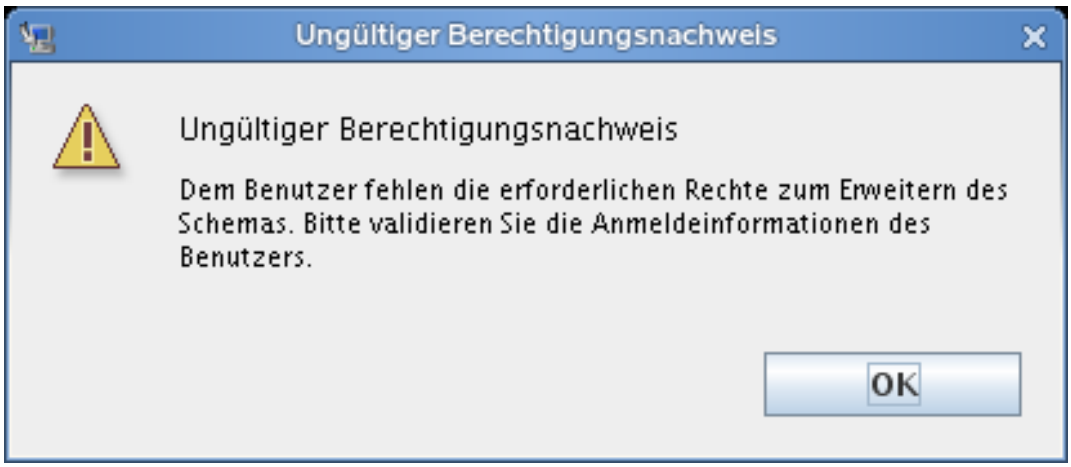
5 Wählen Sie die zu installierenden Komponenten aus und klicken Sie auf *Weiter*. In der Regel werden Sie alle Komponenten installieren.

Der Authentifizierungsbildschirm des Installationsprogramms wird angezeigt:

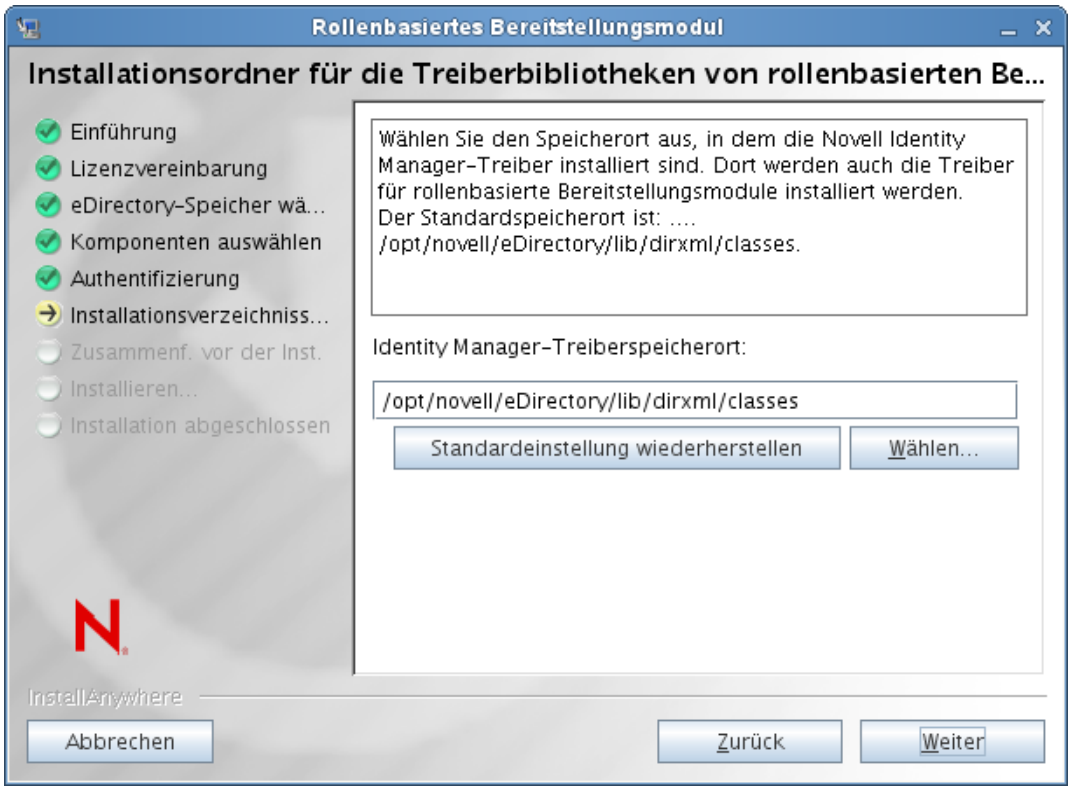


6 Geben Sie den Namen des Administrators im LDAP-Format an und geben Sie das Passwort ein. Geben Sie zudem den Port für den LDAP-Server an.

Falls der Benutzerberechtigungsnachweis ungültig ist oder der Benutzer nicht über die erforderlichen Berechtigungen verfügt, wird eine Fehlermeldung ausgegeben:

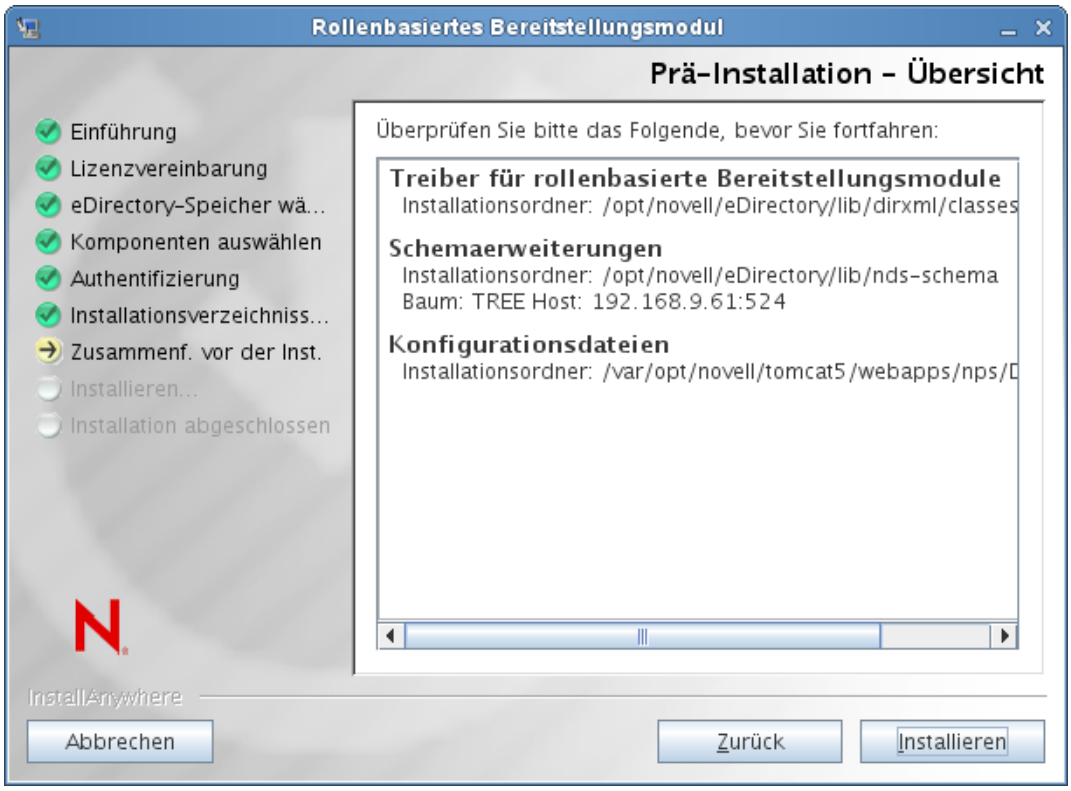

Ungültiger Berechtigungsnachweis
Ungültiger Berechtigungsnachweis
Dem Benutzer fehlen die erforderlichen Rechte zum Erweitern des Schemas. Bitte validieren Sie die Anmeldeinformationen des Benutzers.
OK

Wenn der Benutzerberechtigungsnachweis gültig ist und der Benutzer über die erforderlichen Berechtigungen verfügt, wird der Bildschirm „Installationsordner für die Treiberbibliotheken von rollenbasierten Bereitstellungsmodulen“ angezeigt:



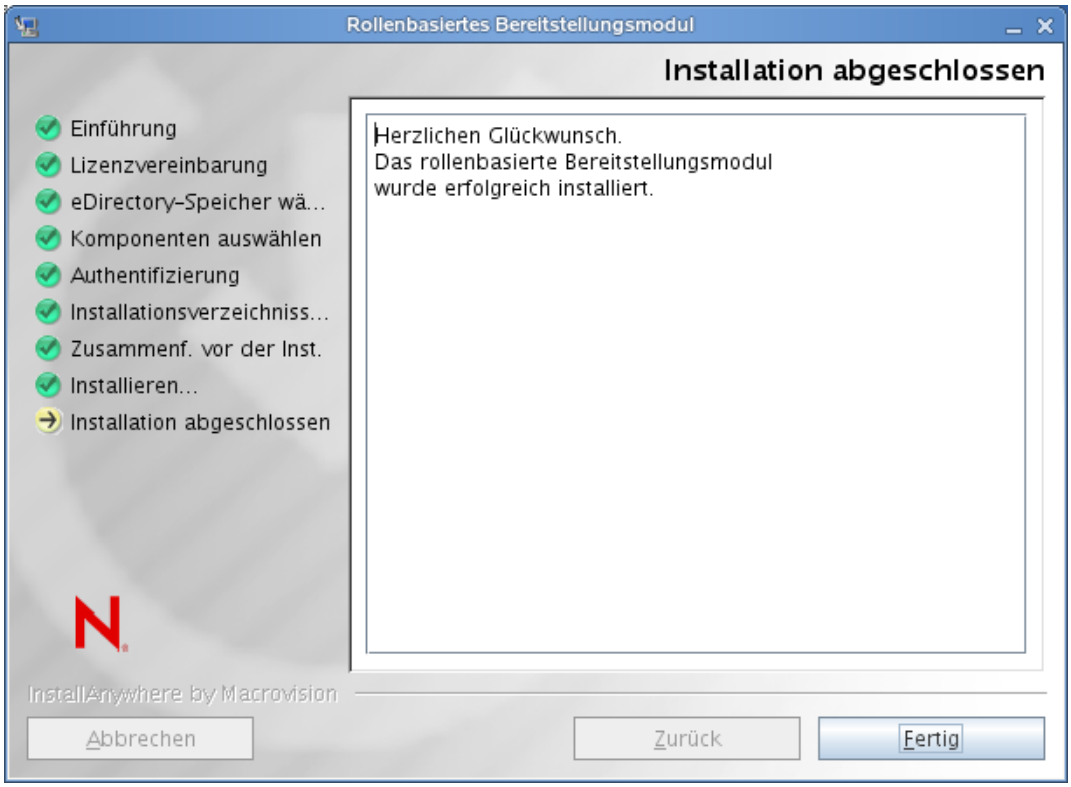
7 Geben Sie den Zielspeicherort auf der Festplatte an, wo die Treiberbibliotheken gespeichert werden sollen, und klicken Sie auf *Weiter*.

Der Bildschirm „Zusammenfassung vor der Installation“ des Installationsprogramms wird angezeigt:



8 Ist die Zusammenfassung korrekt, klicken Sie auf *Installieren*, um den Installationsvorgang zu starten.

Wenn der Installationsvorgang abgeschlossen ist, wird der Bildschirm „Installation abgeschlossen“ des Installationsprogramms angezeigt:



Hinweis: Wenn Sie die mit dem RBPM verknüpften Laufzeitkomponenten deinstallieren müssen, startet das Deinstallationsprogramm Ihren Servercomputer automatisch neu, sofern Sie das Deinstallationsprogramm nicht im Automatikmodus unter Windows ausführen. In diesem Fall müssen Sie Ihren Windows-Computer manuell neu starten. Wenn Sie Identity Manager außerhalb des integrierten Installationsprogramms deinstallieren möchten, müssen Sie darüber hinaus den nds-Dienst anhalten, bevor Sie das Deinstallationsprogramm starten.

3.4 Schema manuell erweitern

Dieser Abschnitt enthält Anweisungen zum manuellen Erweitern des Schemas. Diese Schritte sind nur zum Beheben eines Problems erforderlich, das auftritt, wenn eDirectory nicht am Standardspeicherort installiert ist oder nicht auf den Standard-LDAP-Ports 389 und 636 ausgeführt wird.

So erweitern Sie das Schema manuell (Windows):

1. Beenden Sie eDirectory nach der Installation von Identity Manager.
2. Führen Sie den folgenden Befehl aus, um die in `sch_nt.cfg` aufgelisteten Schemas zu erweitern. Diese Datei befindet sich am Installationsspeicherort von eDirectory.

```
<eDirLocation>\schemaStart.bat <eDirLocation> yes <admin name with tree>
<password> yes 6 " " " <schemafileName>"
"<serverName>" <dibPathLocation>
```

Hinweis: <*dibPathLocation*> muss den DIBFiles-Ordner enthalten.

Im Folgenden finden Sie einen Beispielbefehl:

```
C:\eDir\NDS\schemaStart.bat "C:\eDir\NDS" yes
".cn=admin.o=n.T=IDM-INSTALLISSUE." "n" yes 6 " "
"C:\eDir\NDS\ vrschema.sch" ".CN=WIN2008-64-NDS.O=n.T=IDMINSTALLISSUE."
"C:\DIB\NDS\DIBFiles"
```

Hinweis: Der obige Befehl verwendet sch_nt.cfg nicht zum Erweitern aller Schemadateien, sondern erweitert stattdessen jede einzelne in sch_nt.cfg aufgeführte Schemadatei manuell.

3. Installieren Sie den Rollen- und Ressourcentreiber (wie unter Abschnitt 3.3, „Ausführen des RBPM-Installationsprogramms“, auf Seite 40 beschrieben) bei deaktivierter Option *Schemaerweiterung* im Fenster *Komponenten auswählen*. Schließen Sie die Installation ab.
4. Erweitern Sie nach dem Installieren des Rollen- und Ressourcentreibers die rollenbasierten Schemadateien `srvprv.sch` und `nrf-extensions.sch`, indem Sie den unter Schritt 2 auf Seite 47 aufgelisteten Befehl ausführen.

Hinweis: Dieses Verfahren erweitert die erforderlichen Schemadateien unter Verwendung von `schemaStart.bat`. Dieser Ansatz unterscheidet sich leicht von der Methode, die in der *IDM3.6.1 MetaDirectory Readme* aufgeführt ist.

5. Erweitern Sie das NrfCaseupdate-Schema (`update-nrf-case.sch`) unter Verwendung des Befehls, der unter Schritt 2 auf Seite 47 aufgelistet ist.
6. eDirectory starten.

So erweitern Sie das Schema manuell (SUSE):

1. Installieren Sie den Rollen- und Ressourcentreiber (wie unter Abschnitt 3.3, „Ausführen des RBPM-Installationsprogramms“, auf Seite 40 beschrieben) bei deaktivierter Option *Schemaerweiterung* im Fenster *Komponenten auswählen*. Klicken Sie auf *Weiter*.
2. Wählen Sie einen entsprechenden Installationsspeicherort für den Treiber aus und klicken Sie auf *Weiter*.
3. Wählen Sie einen entsprechenden Installationsspeicherort für die Treiberkonfigurationsdateien aus und klicken Sie auf *Weiter*. Schließen Sie die Installation ab.

   In den Schritten 1 bis 3 werden die Treiber- und Treiberkonfigurationsdateien in den nicht standardmäßigen Speicherort von eDirectory kopiert.
4. Führen Sie den Befehl `ndssch` aus, um das Schema (z. B. `srvprv.sch`, `nrf-extensions.sch`) zu erweitern.

   ```
   ndssch [-h hostname[:port]] [-t tree_name] admin-FDN schemafile...
   ```

   Beispiel:

   ```
   ndssch -h 172.16.1.137:524 -t TESTTREE -p 'PASSWORD'
   .cn=admin.o=novell.T=TESTTREE.
   /opt/novell/eDirectory/lib/nds-schema/srvprv.sch'
   ```
5. Wiederholen Sie Schritt 4, um `nrf-extensions.sch` zu erweitern.

Erstellen der Treiber

4

In diesem Abschnitt wird beschrieben, wie die Treiber zur Verwendung des rollenbasierten Bereitstellungsmoduls (RBPM) erstellt werden. Es werden u. a. folgende Themen erläutert:

- Abschnitt 4.1, „Erstellen der Treiber in Designer“, auf Seite 49

Sie müssen zuerst den Benutzeranwendungstreiber und anschließend den Rollen- und Ressourcenservice-Treiber erstellen. Der Benutzeranwendungstreiber muss zuerst erstellt werden, da der Rollen- und Ressourcenservice-Treiber den Rollendepot-Container (RoleConfig.AppConfig) im Benutzeranwendungstreiber referenziert.

Mit der Treiberkonfigurationsunterstützung können Sie Folgendes ausführen:

- Verknüpfen eines Benutzeranwendungstreibers mit einem Rollen- und Ressourcenservice-Treiber
- Verknüpfen einer Benutzeranwendung mit einem Benutzeranwendungstreiber

---

Wichtig: In dieser Version können Sie den Benutzeranwendungstreiber sowie den Rollen- und Ressourcenservice-Treiber nicht mehr über iManager erstellen. Diese Methode des Erstellens von Treibern wird nicht mehr unterstützt. Zum Erstellen dieser Treiber müssen Sie die neuen Paketverwaltungsfunktionen von Designer verwenden, wie nachfolgend beschrieben.

4.1 Erstellen der Treiber in Designer

Dieser Abschnitt enthält Anweisungen zum Erstellen der Treiber in Designer. Es werden u. a. folgende Themen erläutert:

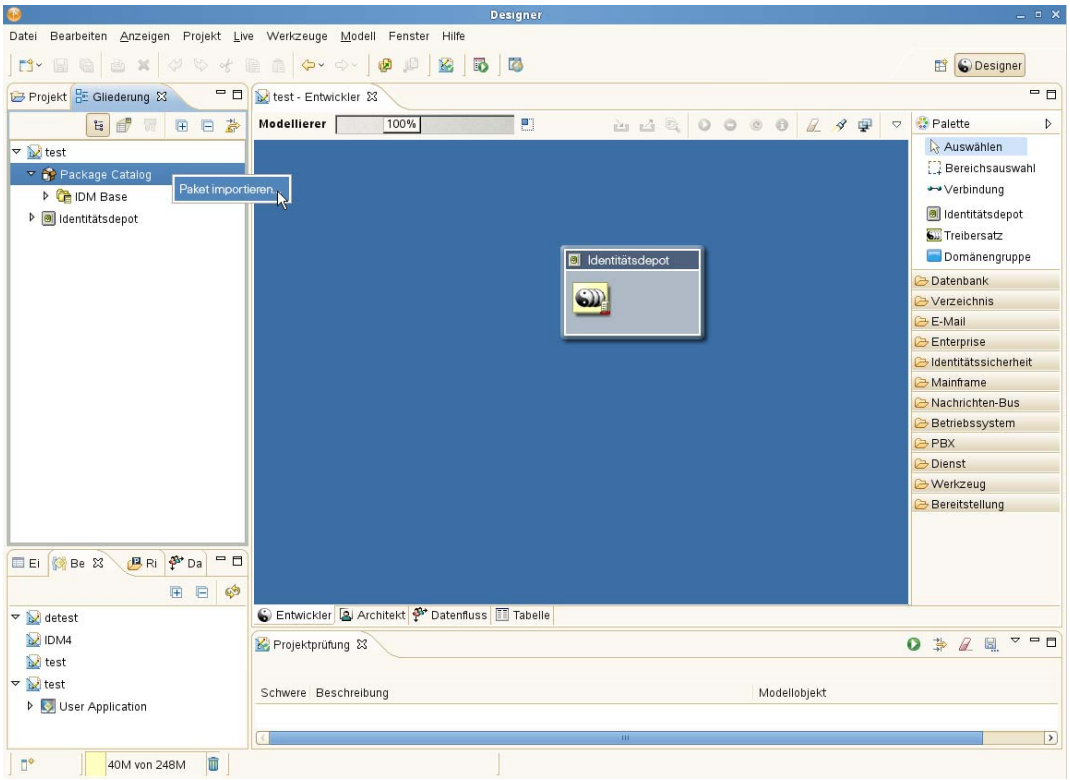
- Abschnitt 4.1.1, „Installieren der Pakete“, auf Seite 49
- Abschnitt 4.1.2, „Erstellen des Benutzeranwendungstreibers in Designer“, auf Seite 51
- Abschnitt 4.1.3, „Erstellen des Rollen- und Ressourcenservice-Treibers in Designer“, auf Seite 55
- Abschnitt 4.1.4, „Bereitstellen der Treiber“, auf Seite 57

4.1.1 Installieren der Pakete

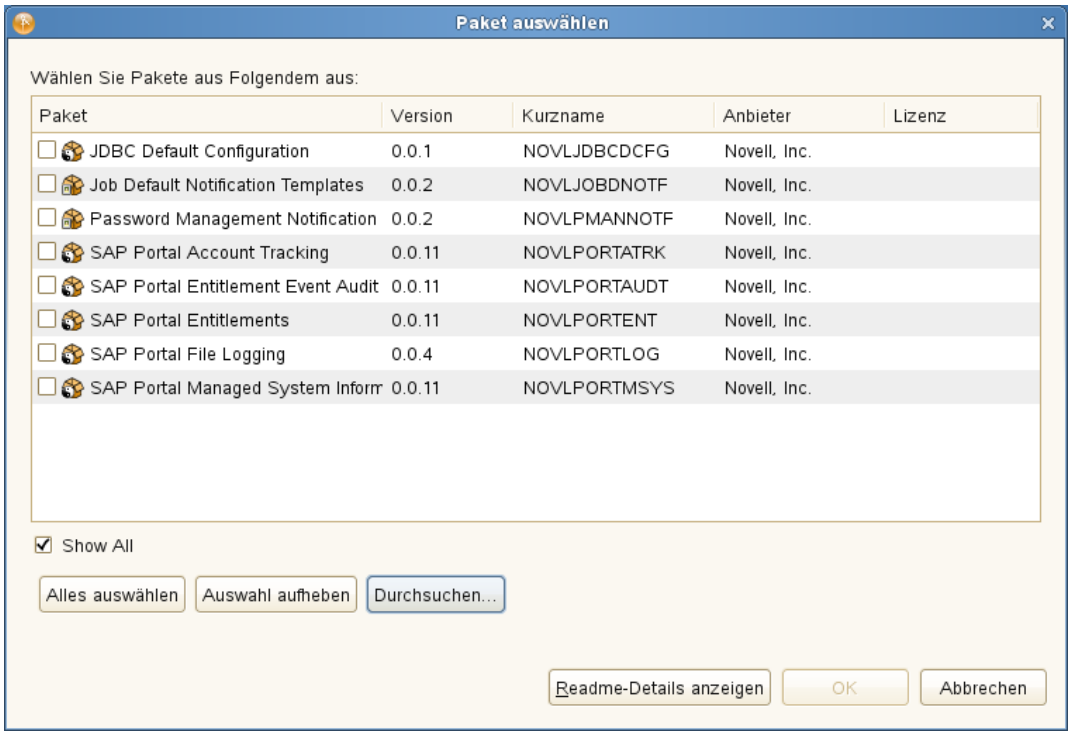
Bevor Sie versuchen, die Treiber zu konfigurieren, müssen Sie sicherstellen, dass Sie alle erforderlichen Pakete im Paketkatalog haben. Wenn Sie ein neues Identity Manager-Projekt erstellen, werden Sie automatisch dazu aufgefordert, mehrere Pakete in das neue Projekt zu importieren. Wenn Sie die Pakete nicht beim Erstellen Ihres Projekts importieren möchten, müssen Sie sie zu einem späteren Zeitpunkt installieren, wie nachfolgend beschrieben.

So installieren Sie die Pakete nach der Erstellung eines neuen Identity Manager-Projekts:

1. Sobald Sie ein neues Identity Manager-Projekt in Designer erstellt haben, wählen Sie den *Paketkatalog* aus und klicken Sie auf *Paket importieren*.



Designer zeigt das Dialogfeld *Paket auswählen* an.


Paket auswählen
Wählen Sie Pakete aus Folgendem aus:
Paket
Version
Kurzname
Anbieter
Lizenz
JDBC Default Configuration 0.0.1 NOVLJDBCDCFG Novell, Inc.
Job Default Notification Templates 0.0.2 NOVLJOBDNOTF Novell, Inc.
Password Management Notification 0.0.2 NOVLPMANNOTF Novell, Inc.
SAP Portal Account Tracking 0.0.11 NOVLPORTATRK Novell, Inc.
SAP Portal Entitlement Event Audit 0.0.11 NOVLPORTAUDT Novell, Inc.
SAP Portal Entitlements 0.0.11 NOVLPORTENT Novell, Inc.
SAP Portal File Logging 0.0.4 NOVLPORTLOG Novell, Inc.
SAP Portal Managed System Inform 0.0.11 NOVLPORTMSYS Novell, Inc.
Show All
Alles auswählen
Auswahl aufheben
Durchsuchen...
Readme-Details anzeigen
OK
Abbrechen

2 Klicken Sie auf *Alle markieren* und anschließend auf *OK*.

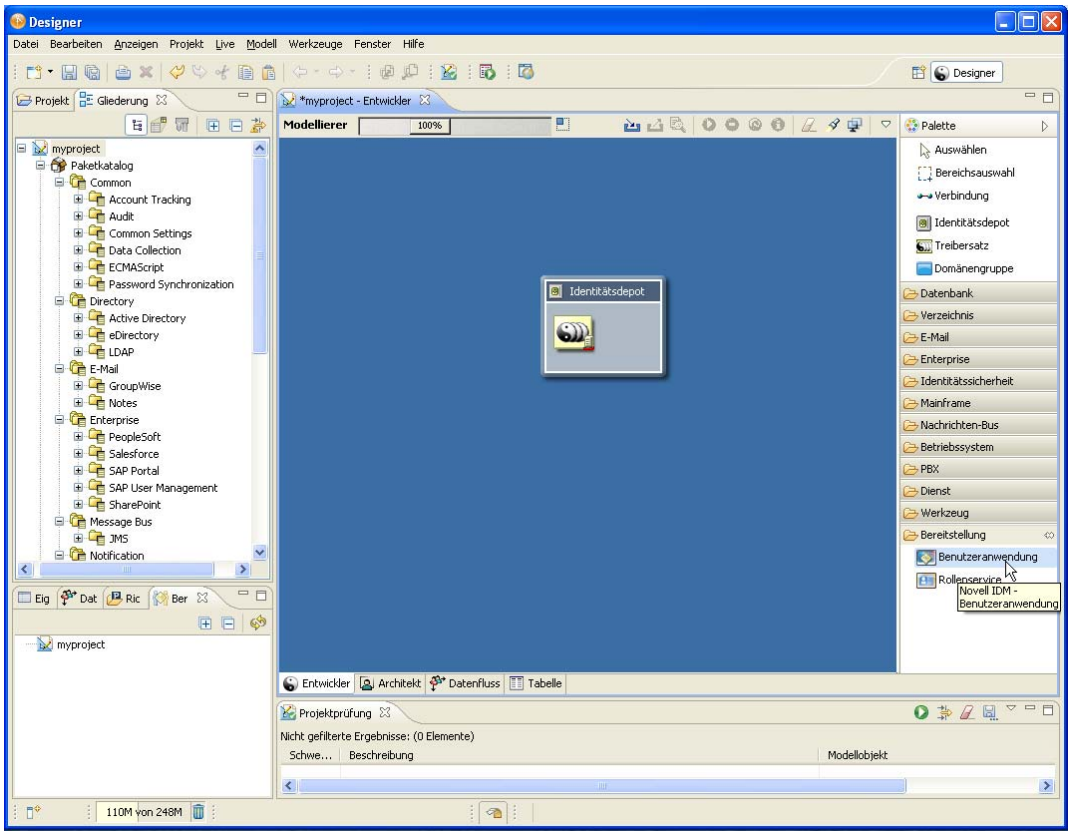
Designer fügt mehrere neue Paketordner unter dem *Paketkatalog* hinzu. Diese Paketordner entsprechen den Objekten in der Palette auf der rechten Seite der Ansicht *Modellierer* in Designer.

3 Klicken Sie auf *Speichern*, um das Projekt zu speichern.

4.1.2 Erstellen des Benutzeranwendungstreibers in Designer

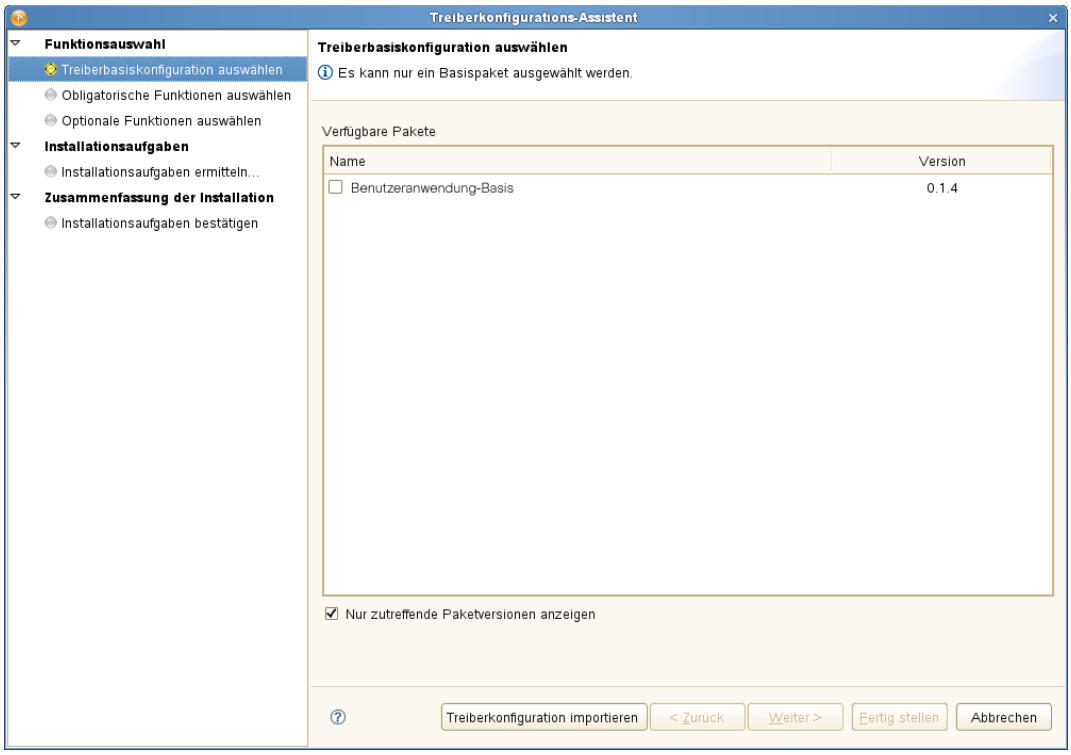
So erstellen Sie den Benutzeranwendungstreiber in Designer:

1 Wählen Sie *Benutzeranwendung* in der Palette der Ansicht *Modellierer* aus:

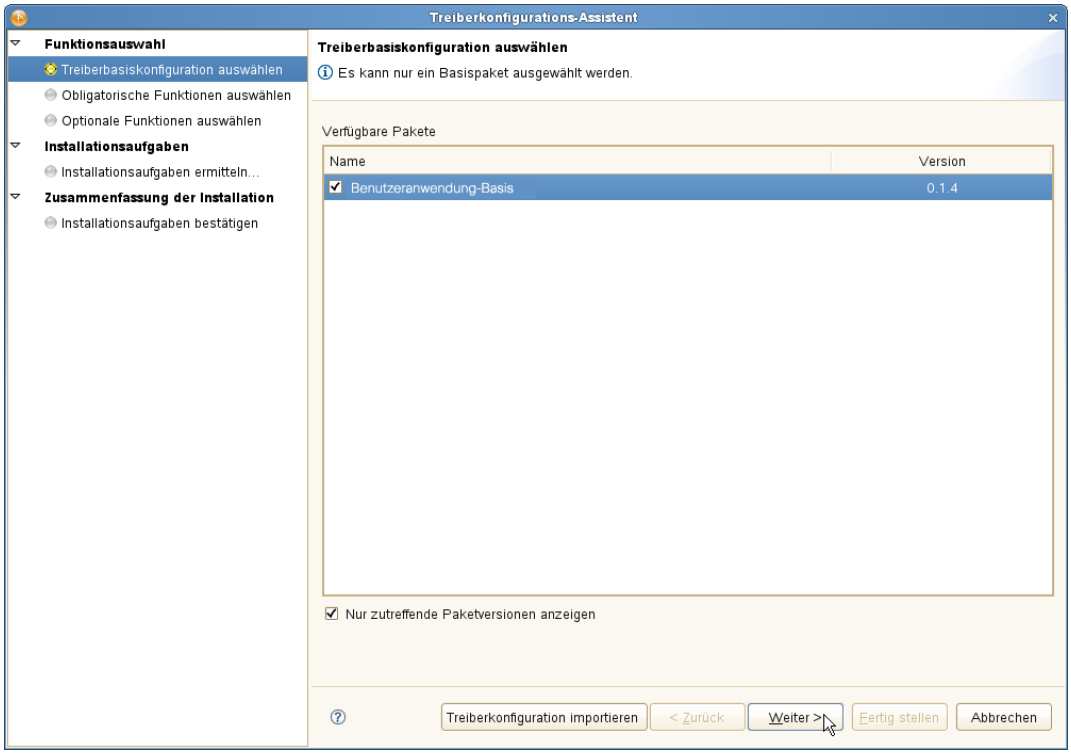


2 Ziehen Sie das Symbol für *Benutzeranwendung* auf die Ansicht *Modellierer.*

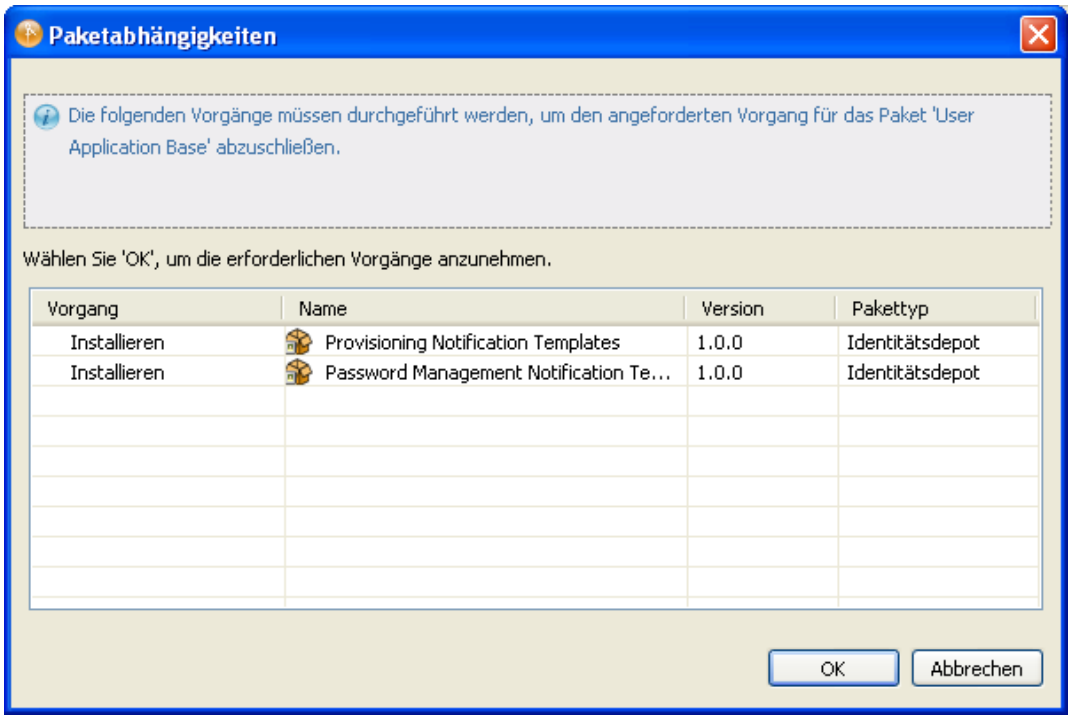
Designer zeigt den *Treiberkonfigurations-Assistenten* an:



3 Wählen Sie *Benutzeranwendungsbasis* und klicken Sie auf *Weiter*:



Auf der Benutzeroberfläche wird ein Dialogfeld angezeigt, das Ihnen mitteilt, dass mehrere zusätzliche Pakete benötigt werden:



4 Klicken Sie auf *OK*, um die erforderlichen Pakete zu installieren.

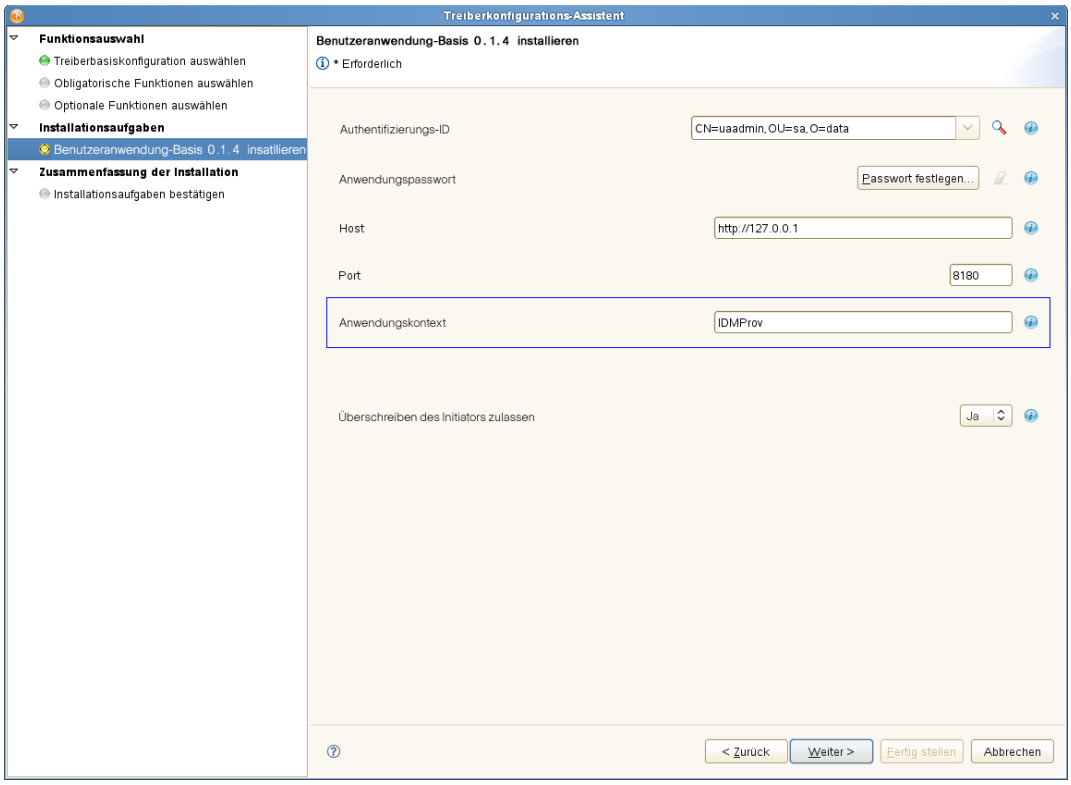
An dieser Stelle zeigt der Assistent einen Bildschirm an, in dem Sie den Namen des Treibers angeben können.

5 Sie können den Standardtreibernamen übernehmen oder einen anderen Namen eingeben.

Drücken Sie *Weiter*.

Der Assistent zeigt jetzt einen Bildschirm an, auf dem Sie die Verbindungsparameter für den Treiber angeben können.

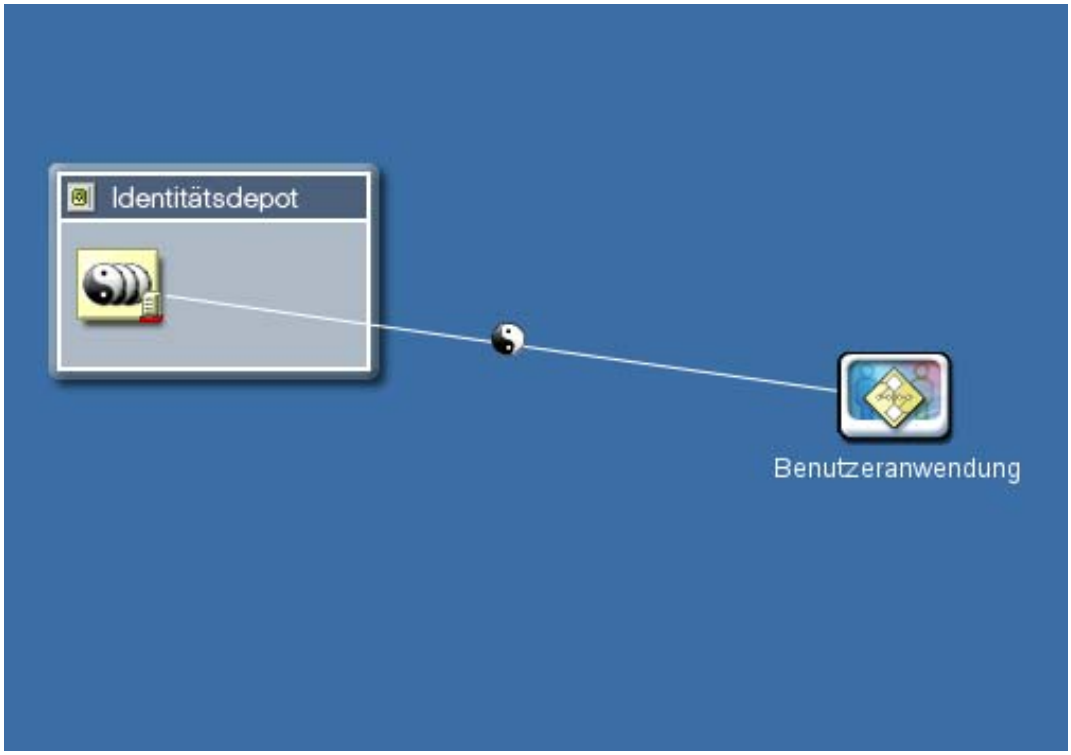
6 Geben Sie die ID und das Passwort für den Benutzeranwendungsadministrator sowie den Host, Port und Anwendungskontext für den Benutzeranwendungs-Server an. Wenn Sie möchten, dass der Bereitstellungsadministrator Workflows im Namen einer anderen Person starten darf, für die der Bereitstellungsadministrator als Vertretung designiert wurde, wählen Sie *Ja* für *Überschreiben des Initiators zulassen*:



Der Assistent zeigt dann den Bildschirm *Installationsaufgaben bestätigen* an.

7 Wenn alle Angaben korrekt sind, klicken Sie auf *Fertig stellen*.

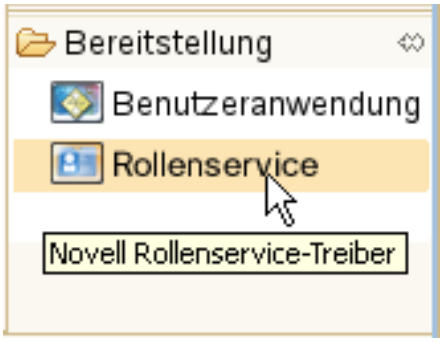
Designer fügt den *Benutzeranwendungstreiber* zur Ansicht *Modellierer* hinzu:



4.1.3 Erstellen des Rollen- und Ressourcenservice-Treibers in Designer

So erstellen Sie den Rollen- und Ressourcenservice-Treiber in Designer:

1. Wählen Sie *Rollenservice* in der Palette der Ansicht *Modellierer* aus:



2. Ziehen Sie das Symbol für *Rollenservice* auf die Ansicht *Modellierer*.

   Designer zeigt den *Treiberkonfigurations-Assistenten* an.

3. Wählen Sie *Rollen- und Ressourcenservice-Basis* aus und klicken Sie auf *Weiter*.

   Der Assistent zeigt einen Bildschirm an, auf dem Sie den Namen des Treibers angeben können.

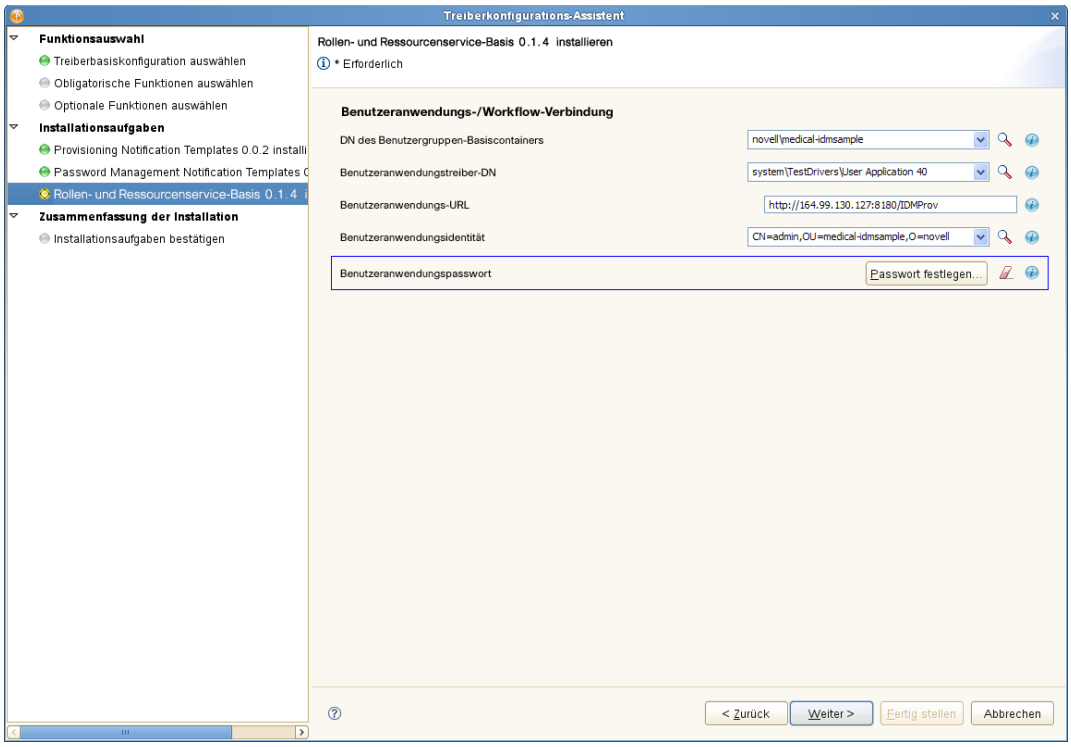
4. Sie können den Standardtreibernamen übernehmen oder einen anderen Namen eingeben.

   Drücken Sie *Weiter*.

   Der Assistent zeigt jetzt einen Bildschirm an, auf dem Sie die Verbindungsparameter für den Treiber angeben können.

5. Geben Sie den DN für den Basiscontainer und den gerade erstellten Benutzeranwendungstreiber an. Da der Treiber noch nicht bereitgestellt wurde, zeigt die Durchsuchen-Funktion den gerade konfigurierten Benutzeranwendungstreiber nicht an. Deshalb müssen Sie den DN für den Treiber eingeben.

   Geben Sie zudem die URL für die Benutzeranwendung zusammen mit der ID und dem Passwort für den Benutzeranwendungsadministrator an:



Klicken Sie auf *Weiter*.

Der Assistent zeigt jetzt den Bildschirm *Installationsaufgaben bestätigen* an.

6 Wenn alle Angaben korrekt sind, klicken Sie auf *Fertig stellen*.

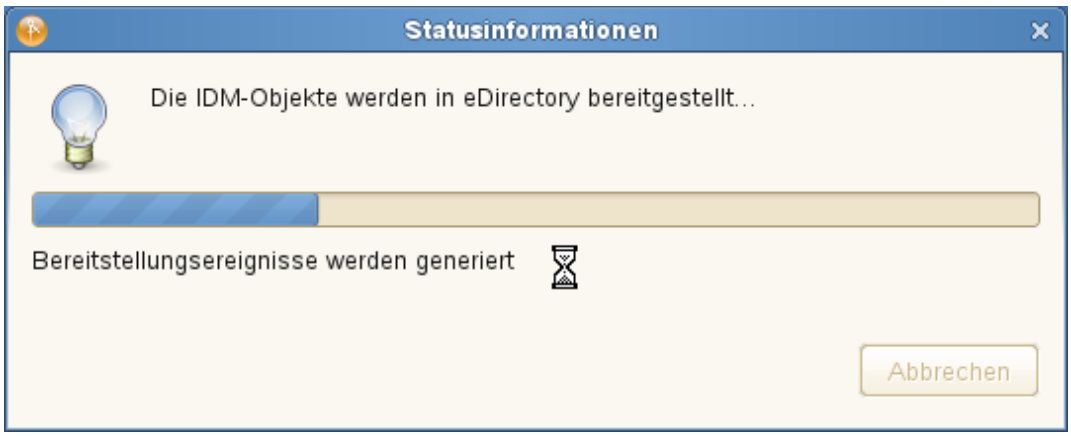
Designer fügt den *Rollenservice*-Treiber zur Ansicht *Modellierer* hinzu:

4.1.4 Bereitstellen der Treiber

So stellen Sie die soeben konfigurierten Treiber bereit:

1. Wählen Sie den Treibersatz (entweder in der Ansicht *Modellierer* oder in der Ansicht *Gliederung*) aus.
2. Wählen Sie *Live* > *Bereitstellen*.

Designer zeigt ein Fortschrittsfenster an, das angibt, welche Objekte bereitgestellt werden:



Wenn der Bereitstellungsprozess abgeschlossen ist, können Sie die Treiber in iManager starten.

Hinweis: Wenn Sie eine eDirectory-Umgebung replizieren, müssen Sie sicherstellen, dass die Reproduktionen das NCP-Server-Objekt für Identity Manager enthalten. Identity Manager ist auf die lokalen Reproduktionen eines Servers beschränkt. Aus diesem Grund startet der Rollen- und Ressourcenservice-Treiber möglicherweise nicht ordnungsgemäß, wenn ein Sekundärserver das Serverobjekt nicht enthält.

Installieren der Benutzeranwendung auf JBoss

5

In diesem Abschnitt wird die Installation der Benutzeranwendung für das rollenbasierte Bereitstellungsmodul auf einem JBoss-Anwendungsserver über die grafische Benutzeroberfläche des Installationsprogramms erläutert. Es werden folgende Themen behandelt:

- Abschnitt 5.1, „Installieren und Konfigurieren der Benutzeranwendungs-WAR“, auf Seite 59
- Abschnitt 5.2, „Testen der Installation“, auf Seite 79

Wenn Sie die Installation lieber über die Befehlszeile durchführen möchten, lesen Sie Kapitel 8, „Installation von der Konsole aus oder mit einem einzigen Befehl“, auf Seite 133.

Installationsprogramm als root-Benutzer ausführen. Sie müssen das Installationsprogramm als root-Benutzer ausführen.

Datenmigration. Weitere Informationen zur Migration finden Sie im *Benutzeranwendung: Migrationshandbuch* (http://www.novell.com/documentation/idm40/index.html).

5.1 Installieren und Konfigurieren der Benutzeranwendungs-WAR

Hinweis: Im Falle von JBoss 5.1.0 benötigt das Installationsprogramm die Java 2 Platform Standard Edition Development Kit Version 1.6 (JRE oder JDK) von Sun. Wenn Sie eine andere Version verwenden, wird die Benutzeranwendungs-WAR-Datei von der Installationsprozedur nicht korrekt konfiguriert. Die Installation scheint erfolgreich zu verlaufen, Sie erhalten aber Fehlermeldungen, wenn Sie die Benutzeranwendung starten.

1 Starten Sie das Installationsprogramm für Ihre Plattform über die Befehlszeile:

Stellen Sie sicher, dass Sie zum Starten des Installationsprogramms für die Benutzeranwendung die korrekte Version der Sun JRE (wie in Abschnitt 1.3, „Systemanforderungen“, auf Seite 12 erläutert) verwenden. Wenn Sie das mit dem rollenbasierten Bereitstellungsmodul mitgelieferte JBossPostgreSQL-Dienstprogramm zum Installieren der JRE verwenden, können Sie mit diesem Befehl das Installationsprogramm starten:

Linux/Solaris

```
$ /opt/novell/jre/bin/java -jar IdmUserApp.jar
```

Windows

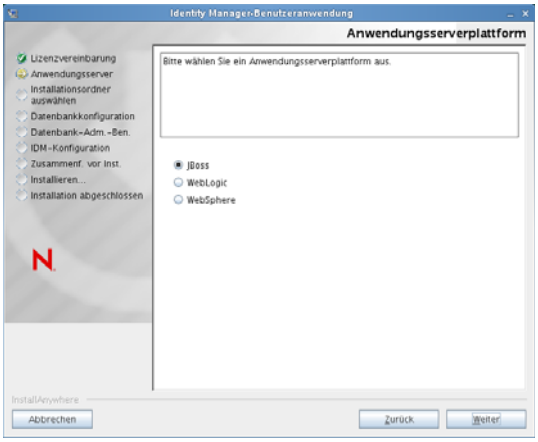
```
C:\Novell\InstallFiles\> "C:\Program Files\Java\jdk1.6.0_14\bin\java.exe"
-jar IdmUserApp.jar
```

Hinweis: SLES-Benutzer: Verwenden Sie nicht das IBM* JDK, das mit SLES mitgeliefert wird. Diese Version ist nicht kompatibel mit einigen Aspekten der Installation und kann den Masterschlüssel beschädigen.

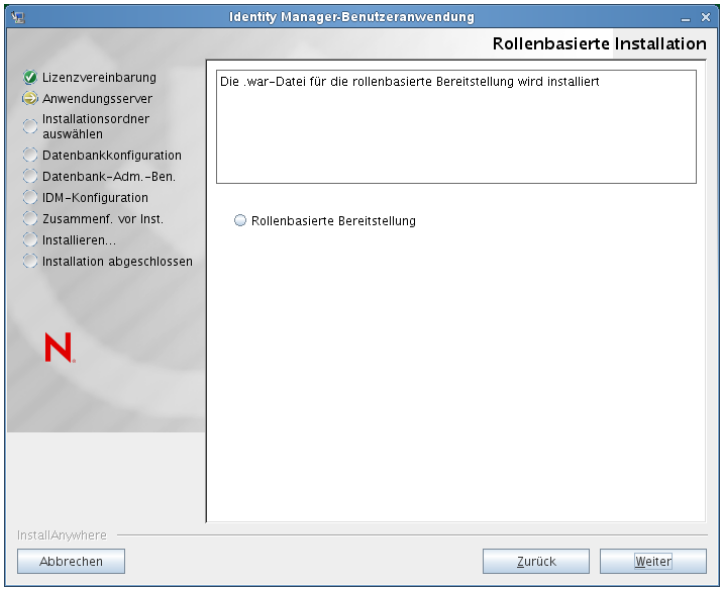
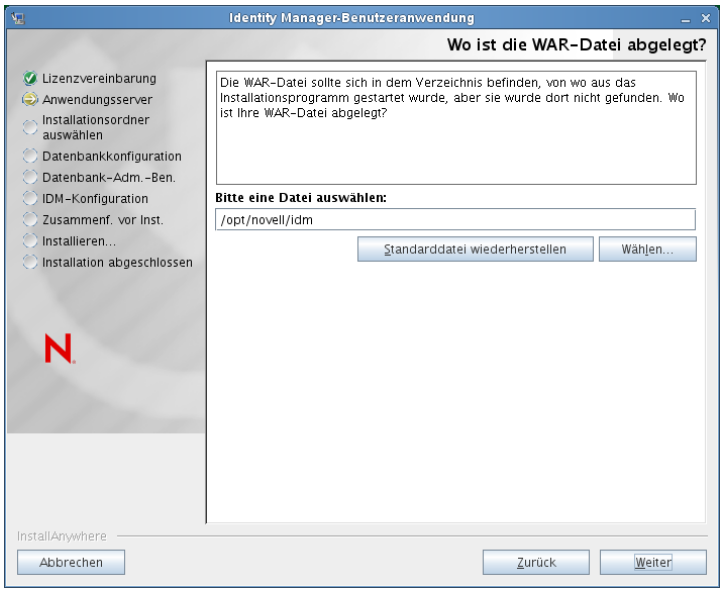
Wenn das Installationsprogramm startet, werden Sie nach der Sprache gefragt:

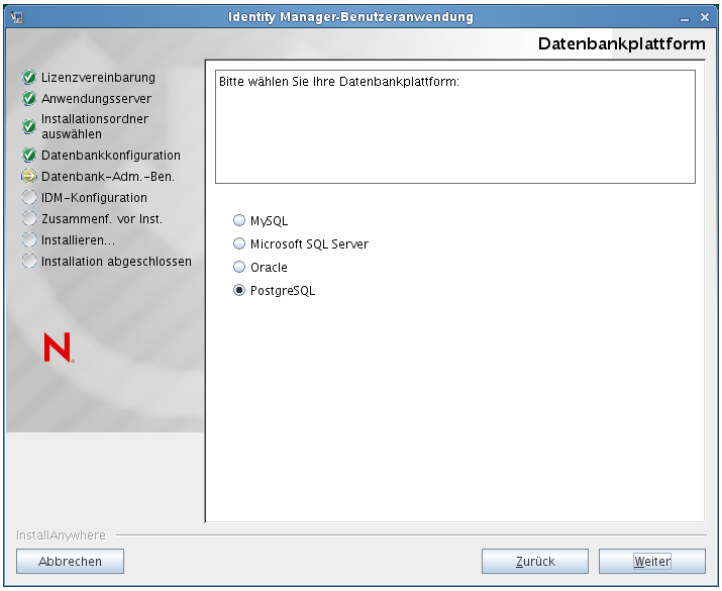
2 Verwenden Sie die nachfolgenden Informationen, um die Sprache auszuwählen, die Lizenzvereinbarung zu akzeptieren und die Anwendungsserverplattform auszuwählen:

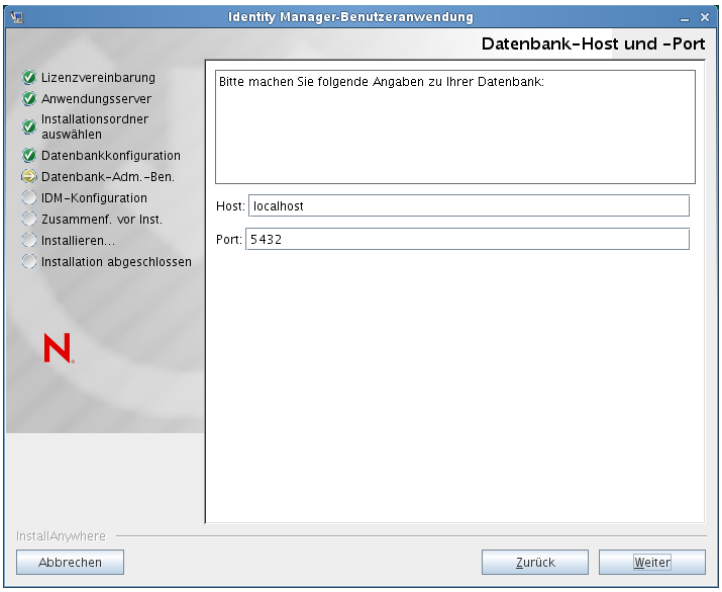
Installationsbildschirm	Beschreibung
Benutzeranwendungsinstallation	Wählen Sie die Sprache für das Installationsprogramm. Die Standardeinstellung ist „Englisch“.
Lizenzvereinbarung	Lesen Sie die Lizenzvereinbarung und klicken Sie auf *Lizenzvertrag zustimmen*.

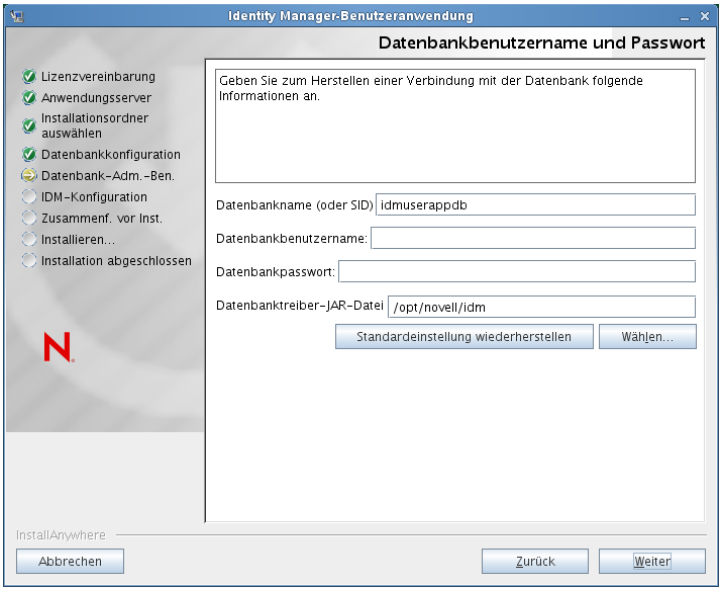
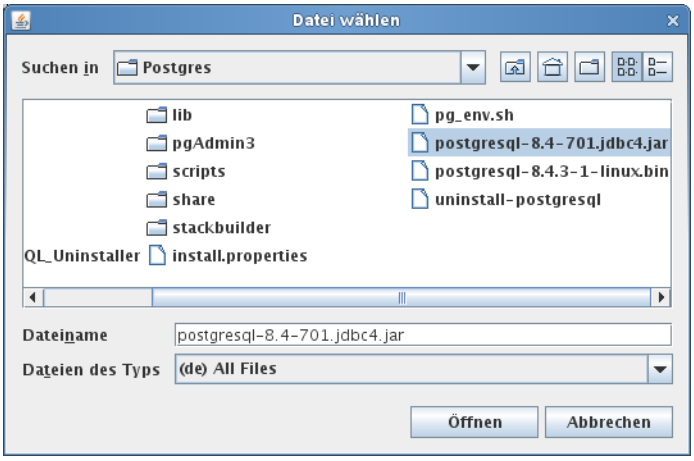
Installationsbildschirm	Beschreibung
Anwendungsserverplattform	Wählen Sie *JBoss*.  Wenn Sie die Installation auf JBoss durchführen, müssen Sie das Installationsprogramm mithilfe der Java-Umgebung von Sun starten. Wenn Sie JBoss als Anwendungsserver wählen und nicht die Java-Umgebung von Sun zum Starten der Installation verwenden, erscheint eine Fehlermeldung und die Installation wird beendet:

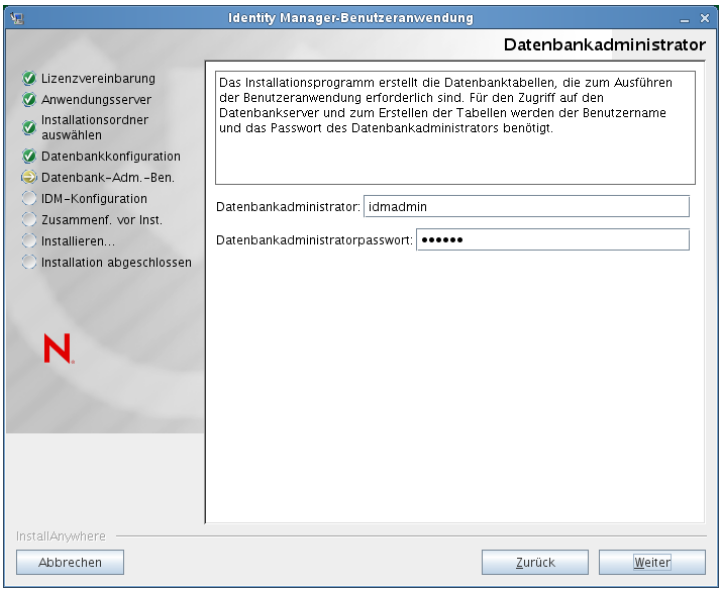
3 Verwenden Sie die nachfolgenden Informationen, um die Installationsart zu wählen, einen Installationsordner auszuwählen und die Datenbank zu konfigurieren:

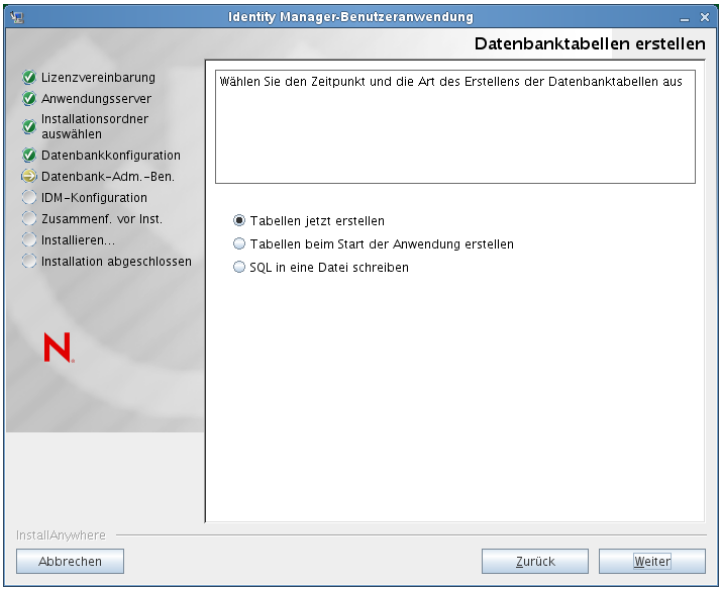
Installationsbildschirm	Beschreibung
Installationstyp	*Rollenbasierte Bereitstellung*: Wählen Sie diese Option aus, um das rollenbasierte Bereitstellungsmodul zu installieren. In dieser Version wird nur diese Installationsart unterstützt. 
Installationsordner auswählen	Geben Sie an, wo das Installationsprogramm die Dateien speichern soll. 

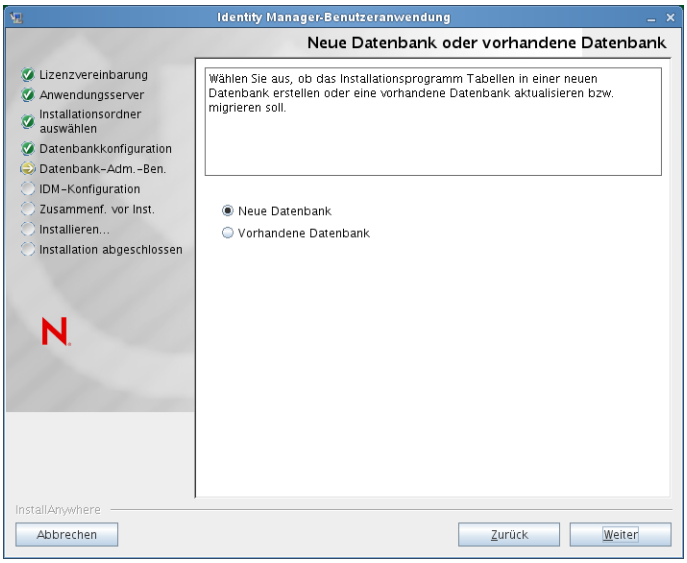
Installationsbildschirm	Beschreibung
Datenbankplattform	Wählen Sie die Datenbankplattform aus:  Die Datenbank- und JDBC-Treiber müssen bereits installiert sein. Für JBoss gibt es folgende Optionen: ◆ MySQL ◆ Microsoft SQL Server ◆ Oracle ◆ PostgreSQL

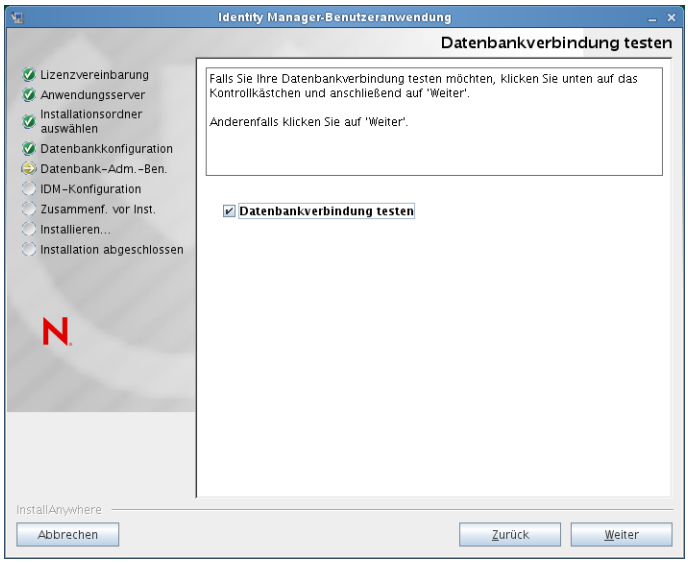
Installationsbildschirm	Beschreibung
Datenbank-Host und Port	*Host*: Geben Sie den Hostnamen oder die IP-Adresse des Datenbankservers an. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied derselbe Hostname bzw. dieselbe IP-Adresse angegeben werden. *Port*: Geben Sie die Listener-Portnummer der Datenbank an. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied derselbe Port angegeben werden. 

Installationsbildschirm	Beschreibung
Datenbankbenutzername und Passwort	*Datenbankname* (oder SID): Geben Sie für PostgreSQL, MySQL oder MS SQL Server den Namen Ihrer Datenbank an. Geben Sie für Oracle den zuvor erstellten Oracle System Identifier (SID) ein. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied derselbe Datenbankname bzw. derselbe SID angegeben werden. Der Standarddatenbankname lautet `idmuserappdb`. *Datenbankbenutzer*name: Geben Sie den Datenbankbenutzer an. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied dieselbe Datenbank angegeben werden. *Datenbankpasswort*: Geben Sie das Datenbankpasswort an. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied dasselbe Passwort angegeben werden. *Datenbanktreiber-JAR-Datei* Geben Sie die Thin-Client-JAR-Datei für den Datenbankserver an. Dieser ist erforderlich.  Wählen Sie für PostgreSQL die Datei „postgresql-8.4-701.jdbc4.jar“ aus: 

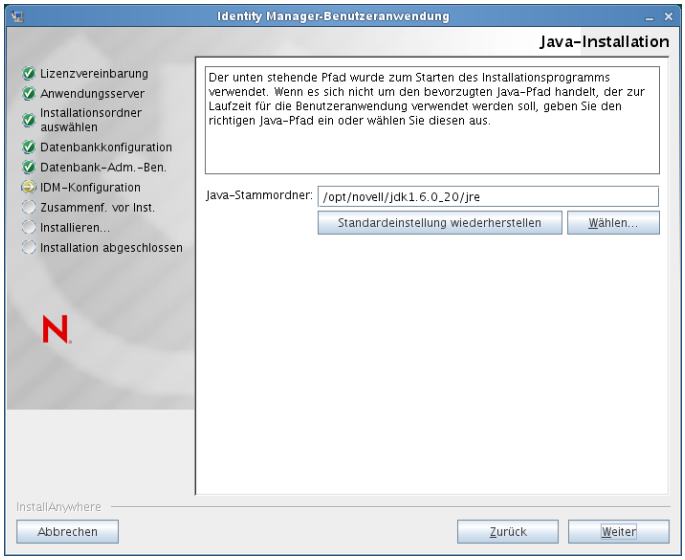
Installationsbildschirm	Beschreibung
Datenbankadministrator	Dieser Bildschirm ist bereits mit dem auf der Seite „Datenbankbenutzername und Passwort“ angegebenen Benutzernamen und Passwort ausgefüllt. Falls der angegebene Datenbankbenutzer nicht über die erforderlichen Berechtigungen zum Erstellen von Tabellen auf dem Datenbankserver verfügt, muss eine andere Benutzer-ID mit den erforderlichen Rechten eingegeben werden. 

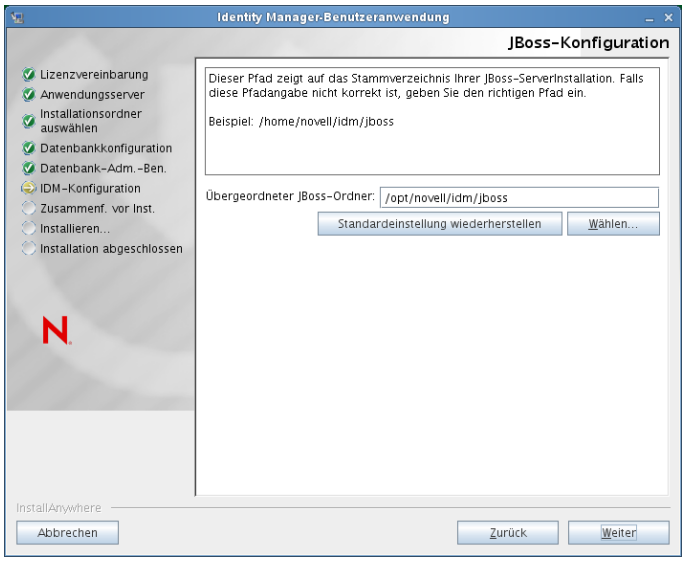
Installationsbildschirm	Beschreibung
Datenbanktabellen erstellen	Geben Sie an, wann die Datenbanktabellen erstellt werden sollen:  Der Bildschirm „Datenbanktabellen erstellen“ enthält die Option zum Erstellen von Tabellen während der Installation oder beim Starten der Anwendung. Ale Alternative dazu können Sie während der Installation eine Schemadatei erstellen, anhand der der Datenbankadministrator später die Tabellen erstellen kann. Wenn Sie eine Schemadatei generieren möchten, aktivieren Sie das Kontrollkästchen *SQL in eine Datei schreiben* und geben Sie im Feld *Schema-Ausgabedatei* einen Namen für die Datei an.

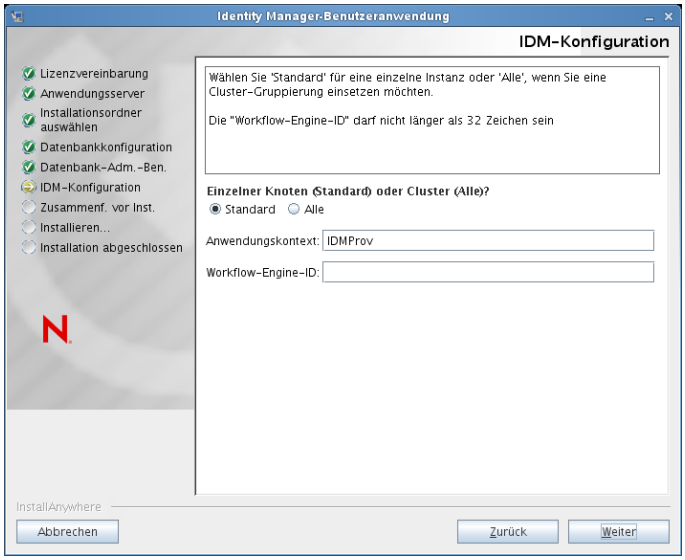
Installationsbildschirm	Beschreibung
Neue Datenbank oder vorhandene Datenbank	Falls die zu verwendende Datenbank neu oder leer ist, klicken Sie auf *Neue Datenbank*. Wenn es sich bei der Datenbank um eine Datenbank einer vorherigen Installation handelt, klicken Sie auf *Vorhandene Datenbank*. 

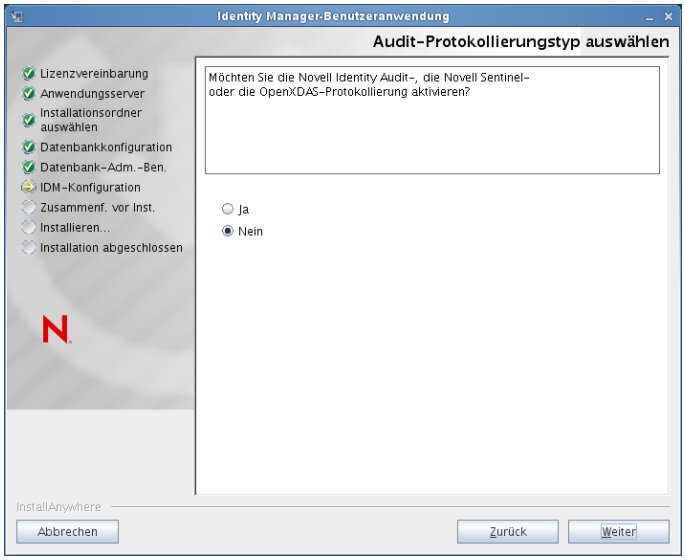
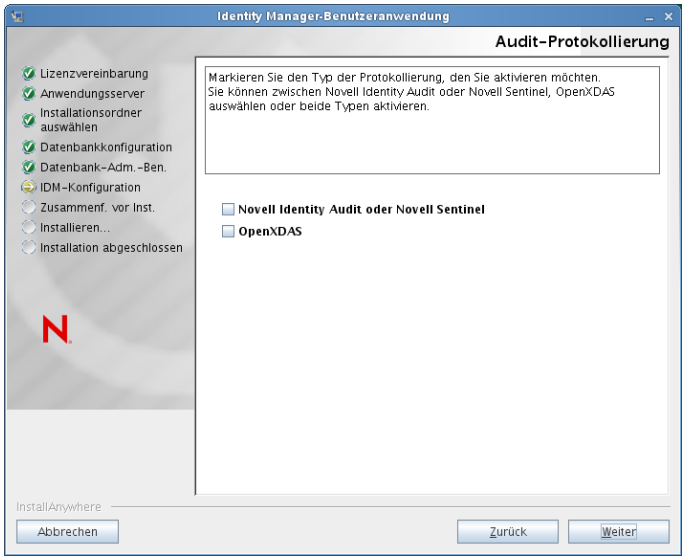
Installationsbildschirm	Beschreibung
Datenbankverbindung testen	Sie können zum Sicherstellen, dass die Informationen in den vorherigen Bildschirmen korrekt sind, die Datenbankverbindung testen, indem Sie das Kontrollkästchen *Datenbankverbindung testen* aktivieren:  Das Installationsprogramm muss sowohl zum direkten Erstellen von Tabellen als auch zum Erstellen der .SQL-Datei eine Verbindung zur Datenbank herstellen. Wenn Sie die Datenbankverbindung testen und der Test fehlschlägt, können Sie dennoch mit der Installation fortfahren. In diesem Fall müssen Sie die Tabellen nach der Installation erstellen, wie im *Benutzeranwendung: Administrationshandbuch* (http://www.novell.com/documentation/idmrbpm40/agpro/?page=/documentation/idmrbpm40/agpro/data/bncf7rj.html) beschrieben.

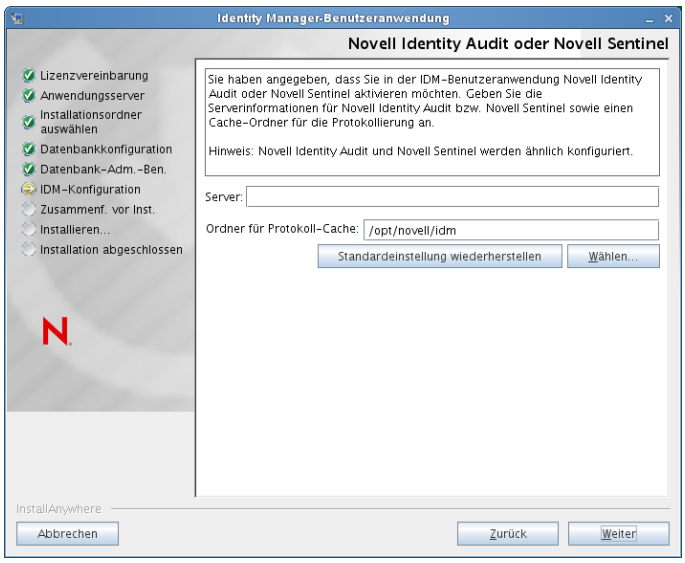
4 Verwenden Sie die nachfolgenden Informationen, um Java, die JBoss-Installation und IDM sowie die Audit-Einstellungen und die Sicherheit zu konfigurieren.

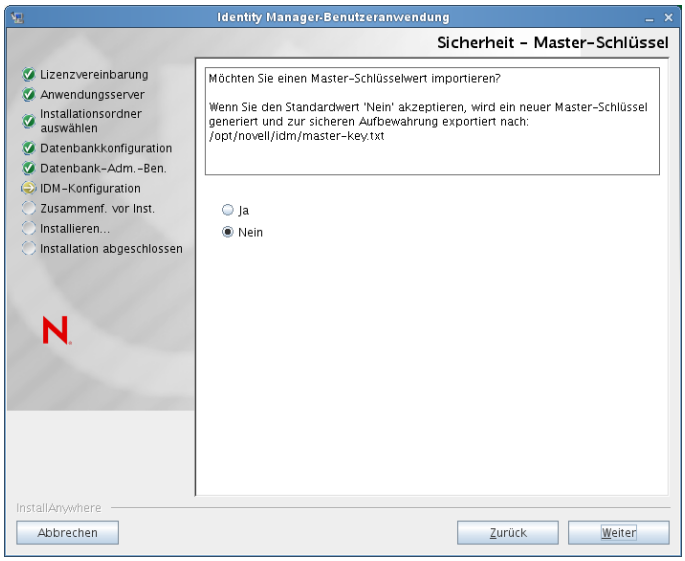
Installationsbildschirm	Beschreibung
Java-Installation	Geben Sie den Java-Stamminstallationsordner an. Die Java-Installation gibt anhand des Werts der Umgebungsvariablen „JAVA_HOME“ den Java-Pfad an und bietet Ihnen die Möglichkeit, den Pfad ggf. zu korrigieren:  Zu diesem Zeitpunkt überprüft das Installationsprogramm, ob die ausgewählte Java-Umgebung für den ausgewählten Anwendungsserver korrekt ist. Zudem wird überprüft, ob das Installationsprogramm in die cacerts-Datei der angegebenen JRE schreiben kann. Anschließend werden Sie gefragt, wo Ihr JBoss-Anwendungsserver installiert ist.

Installationsbildschirm	Beschreibung
JBoss-Konfiguration	Teilt der Benutzeranwendung mit, wo sich der JBoss-Anwendungsserver befindet. Bei diesem Installationsvorgang wird der JBoss-Anwendungsserver nicht installiert. Eine Anleitung für die Installation des JBoss-Anwendungsservers finden Sie in „Installation des JBoss Application Servers und der PostgreSQL-Datenbank“ auf Seite 19. *Übergeordneter JBoss-Ordner*: Geben Sie den Speicherort des JBoss-Anwendungsservers an. 

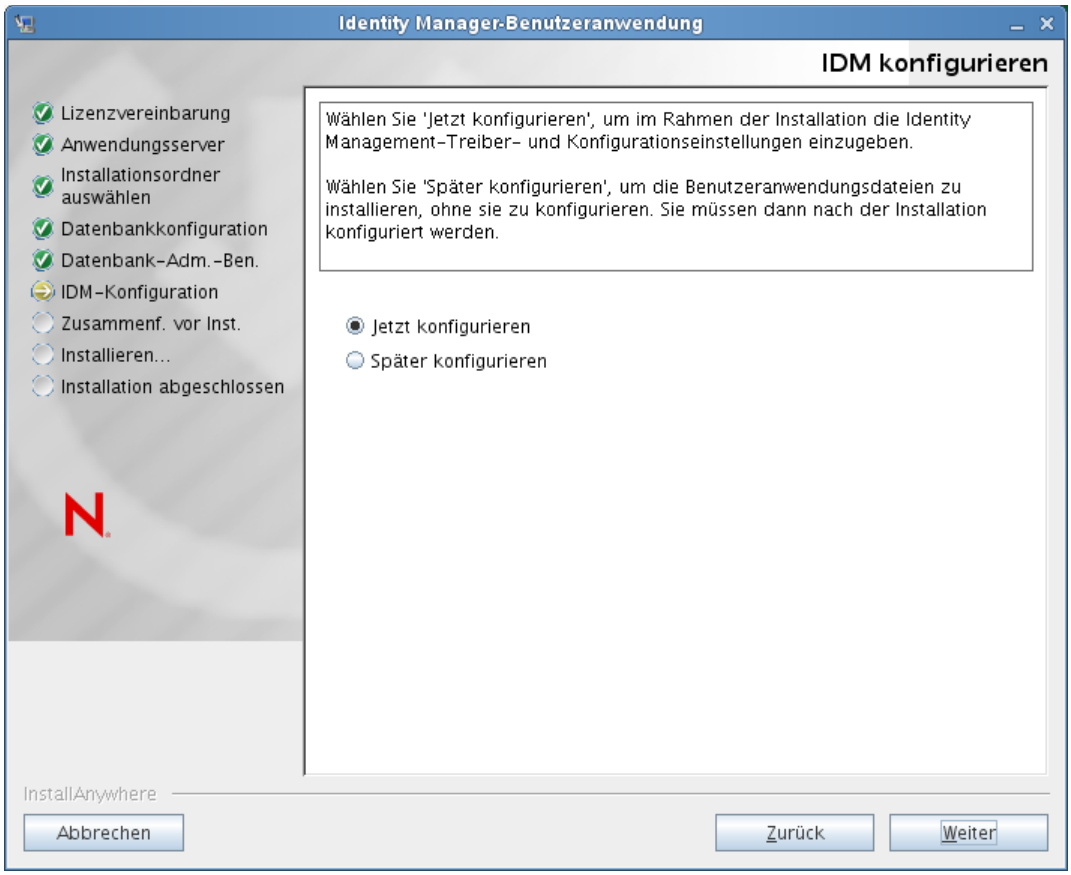
Installationsbildschirm	Beschreibung
IDM-Konfiguration	Wählen Sie den Anwendungsserver-Konfigurationstyp: ◆ Wählen Sie *Standard*, wenn diese Installation für einen einzelnen Knoten erfolgt, der nicht Teil eines Clusters ist. Wenn Sie *Standard* auswählen und zu einem späteren Zeitpunkt einen Cluster benötigen, müssen Sie die Benutzeranwendung erneut installieren. ◆ Wählen Sie *Alle*, wenn diese Installation für ein Cluster erfolgt. *Anwendungskontext*: Der Name der Anwendungsserver-Konfiguration, der Name der WAR-Datei der Anwendung und der Name des URL-Kontexts. Das Installations-Skript erstellt eine Serverkonfiguration und benennt die Konfiguration standardmäßig auf der Basis des *Anwendungsnamens*. Notieren Sie den Anwendungsnamen und fügen Sie ihn in die URL ein, wenn Sie die Benutzeranwendung über einen Browser starten. *Workflow-Engine-ID*: Jeder Server in einem Cluster muss eine eindeutige Workflow-Engine-ID besitzen. Die Workflow-Engine-ID gilt nur für Cluster-Installationen und für den Fall, dass Sie die IDM-Bereitstellungs-War-Datei installieren. Die Engine-ID darf nicht länger als 32 Zeichen sein. Weitere Informationen zu Workflow-Engine-IDs finden Sie im Abschnitt zur Konfiguration von Workflows für das Clustering im *Benutzeranwendung: Administrationshandbuch*. 

Installationsbildschirm	Beschreibung
Audit-Protokollierungstyp auswählen	Klicken Sie auf *Ja*, um die Protokollierung zu aktivieren. Klicken Sie auf *Nein*, um die Protokollierung zu deaktivieren.  Im nächsten Teilfenster werden Sie aufgefordert, den Typ für die Protokollierung anzugeben. Treffen Sie eine Auswahl aus den folgenden Optionen: ◆ *Novell Identity Audit oder Novell Sentinel*: Ermöglicht die Protokollierung über einen Novell-Client für die Benutzeranwendung. ◆ *OpenXDAS*: Ereignisse werden auf Ihrem OpenXDAS-Protokollierungsserver protokolliert. Weitere Informationen zum Einrichten der Protokollierung finden Sie im *Benutzeranwendung: Administrationshandbuch*. 

Installationsbildschirm	Beschreibung
Novell Identity Audit oder Novell Sentinel	*Server*: Geben Sie den Hostnamen oder die IP-Adresse des Servers an, sofern Sie die Protokollierung aktivieren. Wenn Sie die Protokollierung deaktivieren, wird dieser Wert ignoriert. *Ordner für Cache-Protokoll*: Geben Sie das Verzeichnis für den Protokollierungs-Cache-Speicher an. 

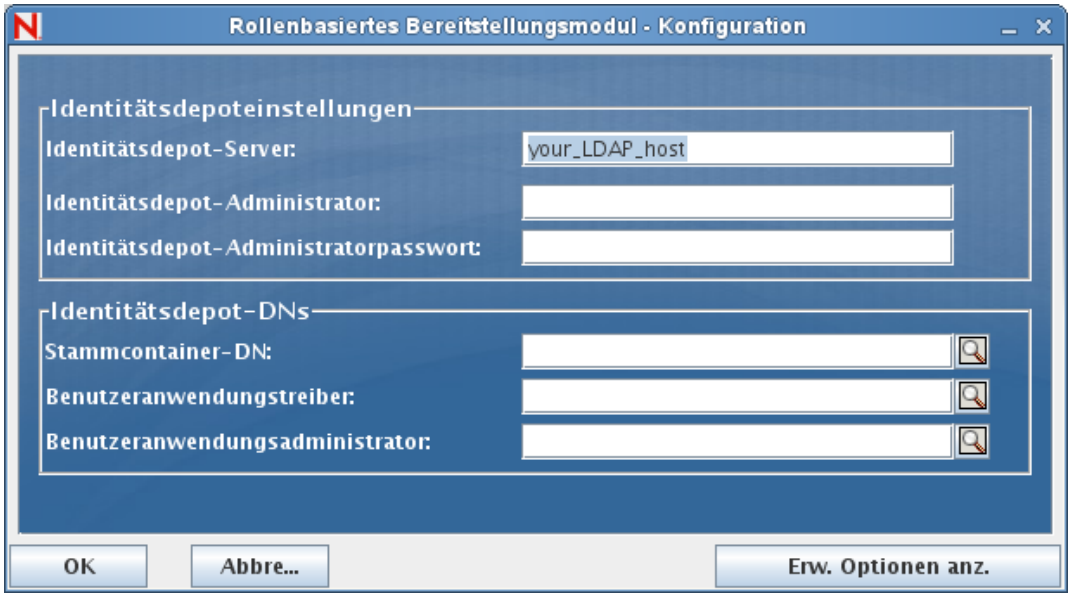
Installationsbildschirm	Beschreibung
Sicherheit - Master-Schlüssel	*Ja*: Erlaubt den Import eines vorhandenen Master-Schlüssels. Wenn ein vorhandener verschlüsselter Master-Schlüssel importiert werden soll, kopieren Sie den Schlüssel und fügen Sie ihn in das Fenster des Installationsvorgangs ein. *Nein*: Erstellt einen neuen Master-Schlüssel. Nach Abschluss der Installation müssen Sie den Master-Schlüssel manuell speichern, wie in Abschnitt 9.1, „Aufzeichnen des Master-Schlüssels“, auf Seite 149 beschrieben.  Bei der Installation wird der verschlüsselte Master-Schlüssel im Installationsverzeichnis in die Datei `master-key.txt` geschrieben. Mögliche Gründe für den Import eines vorhandenen Master-Schlüssels: ◆ Sie verlagern Ihre Installation aus einem Staging-System in ein Produktionssystem und möchten auch weiterhin auf die Datenbank des Staging-Systems zugreifen. ◆ Sie haben die Benutzeranwendung als erstes Mitglied eines JBoss-Clusters installiert und führen nun die Installation auf nachfolgenden Cluster-Mitgliedern durch (für die derselbe Master-Schlüssel benötigt wird). ◆ Bedingt durch einen Festplattenfehler müssen Sie die Benutzeranwendung wiederherstellen. Sie müssen die Benutzeranwendung neu installieren und den Master-Schlüssel der vorherigen Installation angeben. Auf diese Weise erhalten Sie Zugriff auf zuvor gespeicherte verschlüsselte Daten.

5 Wenn Sie RBPM jetzt konfigurieren möchten, wählen Sie *Jetzt konfigurieren* aus und klicken Sie auf *Weiter*.



(Wenn Sie nicht zur Eingabe dieser Informationen aufgefordert werden, haben Sie möglicherweise die in Abschnitt 2.5, „Installieren des Java Development Kit“, auf Seite 32 aufgeführten Schritte nicht ausgeführt.)

Die Standardansicht des Konfigurationsfensters für das rollenbasierte Bereitstellungsmodul enthält diese sechs Felder:



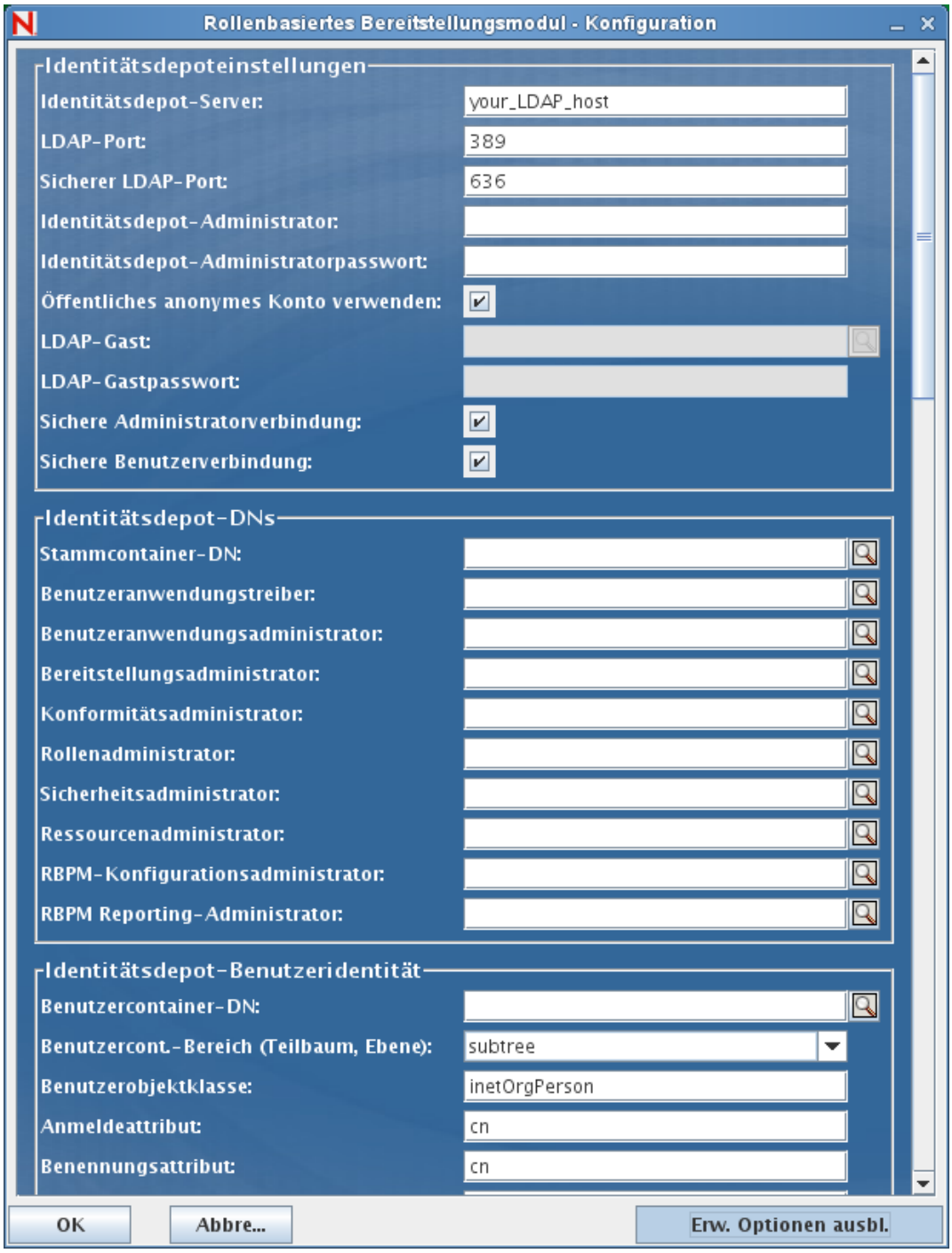
Das Installationsprogramm übernimmt den Wert aus der Stammcontainer-DN und wendet ihn auf die folgenden Werte an:

- Benutzercontainer-DN
- Gruppencontainer-DN

Das Installationsprogramm übernimmt den Wert aus den Benutzeranwendungsadministratorfeldern und wendet ihn auf die folgenden Werte an:

- Bereitstellungsadministrator
- Konformitätsadministrator
- Rollenadministrator
- Sicherheitsadministrator
- Ressourcenadministrator
- RBPM-Konfigurationsadministrator

Wenn Sie diese Werte explizit angeben möchten, klicken Sie auf *Erweiterte Optionen anzeigen* und ändern Sie sie:



Bei der Installation der Benutzeranwendung können Sie Konfigurationsparameter für die Benutzeranwendung festlegen. Die meisten dieser Parameter können auch nach der Installation in der Datei `configupdate.sh` oder `configupdate.bat` bearbeitet werden. Auf Ausnahmen wird in den Parameterbeschreibungen hingewiesen.

Unter Anhang A, „IDM Benutzeranwendung - Konfigurationsreferenz“, auf Seite 157 finden Sie eine Beschreibung für jede Option.

6 Mithilfe der folgenden Informationen wird die Installation ausgeführt.

Installationsbildschirm	Beschreibung
Zusammenfassung vor der Installation	Überprüfen Sie auf der Seite „Zusammenfassung vor der Installation“ die Einstellungen der Installationsparameter. Wenn Sie Änderungen vornehmen möchten, können Sie über die Schaltfläche *Zurück* vorherige Installationsseiten aufrufen. Die Werte auf der Seite „Benutzeranwendung - Konfiguration“ werden nicht gespeichert, daher müssen Sie die Einstellungen auf dieser Seite erneut vornehmen, wenn Sie vorherige Seiten des Installationsvorgangs ändern. Wenn Sie die gewünschten Änderungen an den Installations- und Konfigurationsparametern vorgenommen haben, kehren Sie zur Seite „Zusammenfassung vor der Installation“ zurück und klicken Sie auf *Installieren*.
Installation abgeschlossen	Zeigt an, dass die Installation abgeschlossen ist.

Installationsprogramm erstellt novlua-Benutzer. Das Installationsprogramm erstellt einen neuen Benutzer mit dem Namen „novlua“. Das jboss_init-Skript führt JBoss als dieser Benutzer aus und die definierten Berechtigungen in den JBoss-Dateien sind auf diesen Benutzer festgelegt.

5.1.1 Anzeigen der Installations- und Protokolldateien

Wenn die Installation ohne Fehler abgeschlossen wurde, fahren Sie mit Testen der Installation fort. Sofern bei der Installation Fehler- oder Warnmeldungen ausgegeben wurden, ermitteln Sie die Probleme anhand der Protokolldateien:

- Die Datei `Identity_Manager_User_Application_InstallLog.log` enthält die Ergebnisse der wichtigsten Installationsaufgaben.
- Die Datei `Novell-Custom-Install.log` enthält Informationen zur Konfiguration der Benutzeranwendung, die während der Installation vorgenommen wurde.

5.2 Testen der Installation

1. Starten Sie die Datenbank. Eine Anleitung hierzu finden Sie in der Dokumentation zur Datenbank.
2. Starten Sie den Benutzeranwendungsserver (JBoss). Wechseln Sie an der Befehlszeile zum Installationsverzeichnis und führen Sie das folgende Skript aus (bereitgestellt von der Benutzeranwendungs-Installation):

   `/etc/init.d/jboss_init start` (Linux und Solaris)

   `start-jboss.bat` (Windows)

   Wenn Sie den Anwendungsserver nicht auf einem X11 Window System ausführen, müssen Sie das Flag - `Djava.awt.headless=true` in Ihr Server-Startskript einfügen. Dies ist nicht für das Ausführen von Berichten erforderlich. Sie können beispielsweise folgende Zeile zu Ihrem Skript hinzufügen:

   ```
   JAVA_OPTS="-Djava.awt.headless=true -server -Xms256M -Xmx256M-
   XX:MaxPermSize=256m"
   ```

3 Starten Sie den Benutzeranwendungstreiber. So wird die Kommunikation mit dem Benutzeranwendungstreiber ermöglicht.

   3a Melden Sie sich bei iManager an.

   3b Wählen Sie in der Anzeige der Rollen und Aufgaben im linken Navigationsrahmen unter *Identity Manager* die Option *Identity Manager-Überblick*.

   3c Geben Sie im angezeigten Inhaltsrahmen den Treibersatz ein, der den Benutzeranwendungstreiber enthält, und klicken Sie auf *Suchen*. Es wird eine Grafik aufgerufen, in der der Treibersatz mit seinen verknüpften Treibern angezeigt wird.

   3d Klicken Sie auf dem Treiber auf das rot-weiße Symbol.

   3e Wählen Sie *Treiber starten*. Der Treiberstatus ändert sich in das Yin-Yang-Symbol, das anzeigt, das der Treiber gestartet wurde.

   Beim Start versucht der Treiber mit der Benutzeranwendung einen „Handshake“ durchzuführen. Wenn die Benutzeranwendung nicht läuft oder die WAR-Datei nicht erfolgreich bereitgestellt wurde, gibt der Treiber einen Fehler zurück.

4 Sie können die Benutzeranwendung starten und sich bei ihr anmelden, indem Sie im Adressfeld Ihres Webbrowsers folgende URL angeben:

   http://*Hostname*:*Port*/*Anwendungsname*

   In dieser URL entspricht *Hostname*:*Port* dem Hostnamen des Anwendungsservers (z. B. MeinServer.Domäne.com) und dem Port des Anwendungsservers (der Standard-Port auf JBoss ist beispielsweise Port 8180). *Anwendungsname* ist standardmäßig *IDMProv*. Der Anwendungsname wurde während der Installation bei der Eingabe der Konfigurationsinformationen für den Anwendungsserver angegeben.

   Die Standard-Portalseite der Novell Identity Manager-Benutzeranwendung wird angezeigt.

5 Klicken Sie am oberen rechten Seitenrand auf *Anmelden*, um sich bei der Benutzeranwendung anzumelden.

Wird nach Ausführung dieser Schritte die Seite „Identity Manager-Benutzeranwendung“ nicht im Browser angezeigt, überprüfen Sie die Terminal-Konsole auf Fehlermeldungen und lesen Sie in Abschnitt 9.9, „Fehlersuche“, auf Seite 155 nach.

Installieren der Benutzeranwendung auf WebSphere

6

In diesem Abschnitt wird die Installation der Benutzeranwendung für das rollenbasierte Bereitstellungsmodul auf einem WebSphere-Anwendungsserver über die grafische Benutzeroberfläche des Installationsprogramms erläutert.

- Abschnitt 6.1, „Installieren und Konfigurieren der Benutzeranwendungs-WAR“, auf Seite 81
- Abschnitt 6.2, „Konfigurieren der WebSphere-Umgebung“, auf Seite 96
- Abschnitt 6.3, „Bereitstellung der WAR-Datei“, auf Seite 111
- Abschnitt 6.4, „Starten der und Zugriff auf die Benutzeranwendung“, auf Seite 112

Führen Sie das Installationsprogramm als Nicht-root-Benutzer aus.

Datenmigration. Weitere Informationen zur Migration finden Sie im *Benutzeranwendung: Migrationshandbuch* (http://www.novell.com/documentation/idm40/index.html).

6.1 Installieren und Konfigurieren der Benutzeranwendungs-WAR

Hinweis: Für WebSphere 7.0 benötigt das Installationsprogramm das JDK 1.6 Version 1.6 von IBM. Falls Sie eine andere Version verwenden, wird die Benutzeranwendungs-WAR-Datei nicht erfolgreich konfiguriert. Die Installation scheint erfolgreich zu verlaufen, Sie erhalten aber Fehlermeldungen, wenn Sie die Benutzeranwendung starten.

1. Rufen Sie das Verzeichnis mit den Installationsdateien auf.
2. Sie müssen die uneingeschränkten Richtliniendateien auf die IBM JDK anwenden. In der WebSphere-Dokumentation gibt es einen Link auf diese Dateien von IBM sowie auf Anweisungen, wie sie anzuwenden sind. Wenden Sie diese Dateien auf Ihre IBM JDK-Umgebung an, bevor Sie mit der Installation fortfahren. Die JAR-Datei für uneingeschränkte Richtliniendateien muss unter „JAVA_HOME\jre\lib\security“ gespeichert werden.

   Ohne diese uneingeschränkten Richtliniendateien erhalten Sie die Fehlermeldung „Ungültige Schlüsselgröße“. Die Hauptursache dieses Problems ist der Mangel an uneingeschränkten Richtliniendateien. Stellen Sie also sicher, dass Sie das richtige IBM JDK verwenden.
3. Starten Sie das Installationsprogramm mithilfe der IBM Java-Umgebung, wie nachfolgend dargestellt:

   Linux oder Solaris

   ```
   $ /opt/WS/IBM/WebSphere/AppServer/java/bin/java -jar IdmUserApp.jar
   ```

   Windows

   ```
   C:\WS\IBM\WebSphere\AppServer\java\bin\java -jar IdmUserApp.jar
   ```

   Wenn das Installationsprogramm startet, werden Sie nach der Sprache gefragt:

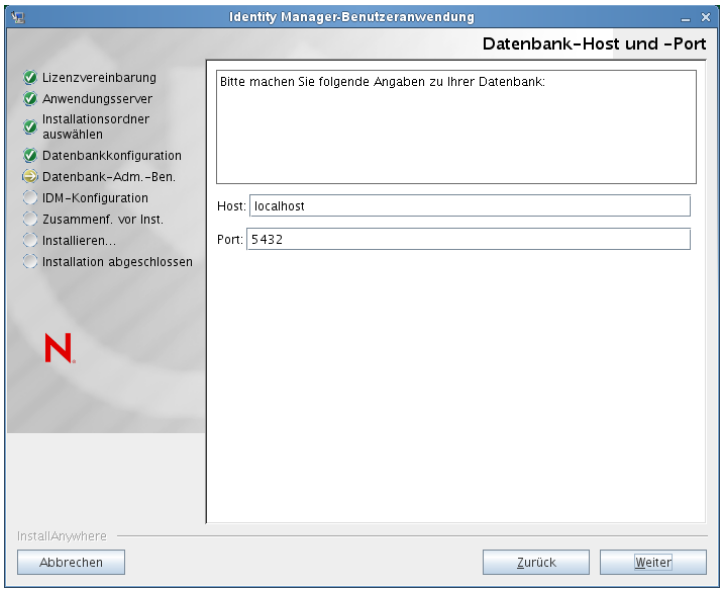
4 Verwenden Sie die nachfolgenden Informationen, um die Sprache auszuwählen, die Lizenzvereinbarung zu akzeptieren und die Anwendungsserverplattform auszuwählen:

Installationsbildschirm	Beschreibung
Benutzeranwendungsinstallation	Wählen Sie die Sprache für das Installationsprogramm. Die Standardeinstellung ist „Englisch“.
Lizenzvereinbarung	Lesen Sie die Lizenzvereinbarung und klicken Sie auf *Lizenzvertrag zustimmen*.

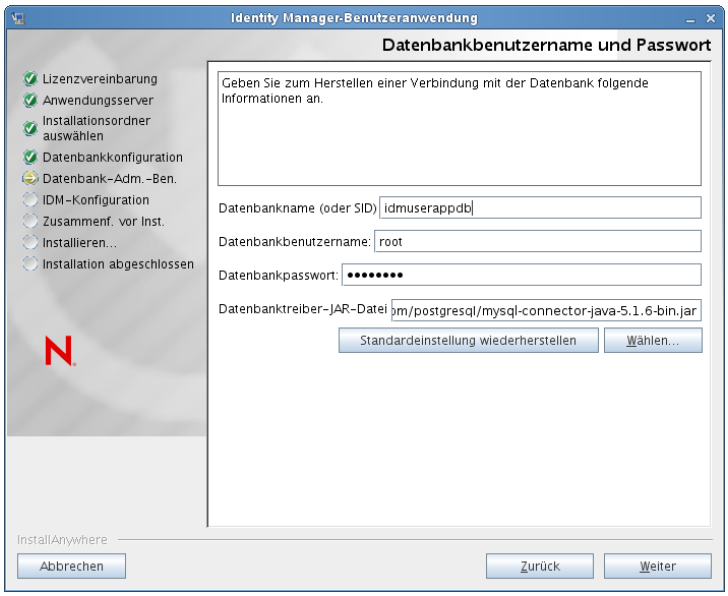
Installationsbildschirm	Beschreibung
Anwendungsserverplattform	Wählen Sie *WebSphere*. Wenn sich die WAR-Datei der Benutzeranwendung nicht im selben Verzeichnis befindet wie das Installationsprogramm, werden Sie aufgefordert, den Pfad zur WAR-Datei einzugeben. Wenn sich die WAR-Datei am Standardspeicherort befindet, können Sie auf *Standarddatei wiederherstellen* klicken. Sie können stattdessen auch auf die Schaltfläche zum *Auswählen* klicken und einen Speicherort auswählen, um den Speicherort der WAR-Datei anzugeben. Wenn Sie die Installation auf WebSphere durchführen, müssen Sie das Installationsprogramm mithilfe der Java-Umgebung von IBM starten. Wenn Sie WebSphere als Anwendungsserver wählen und nicht die Java-Umgebung von IBM zum Starten der Installation verwenden, erscheint eine Fehlermeldung und die Installation wird beendet:

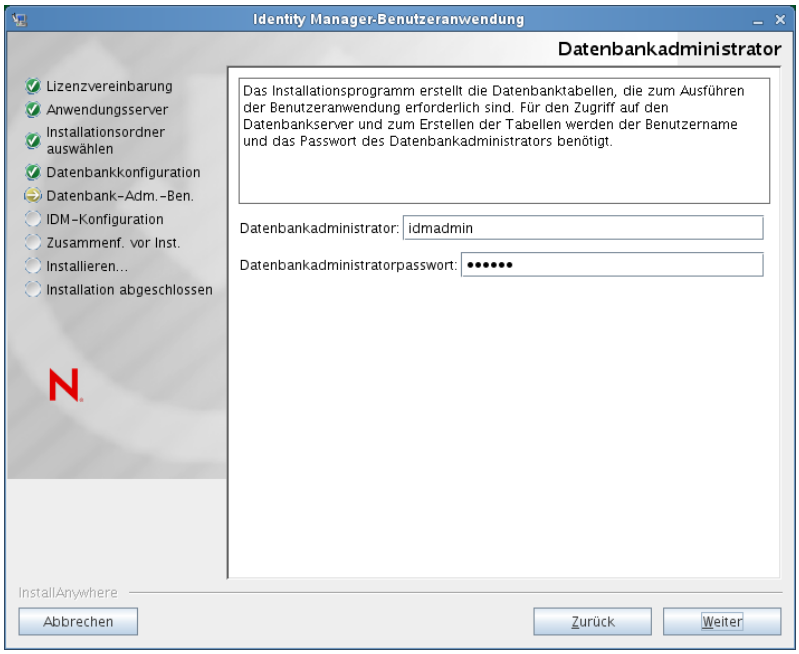
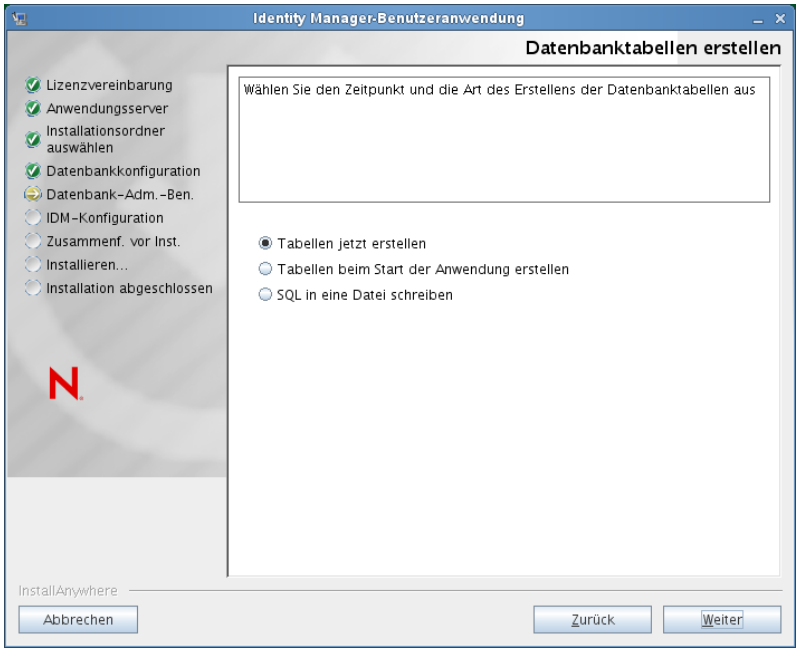
5 Verwenden Sie die nachfolgenden Informationen, um die Installationsart zu wählen, einen Installationsordner auszuwählen und die Datenbank zu konfigurieren:

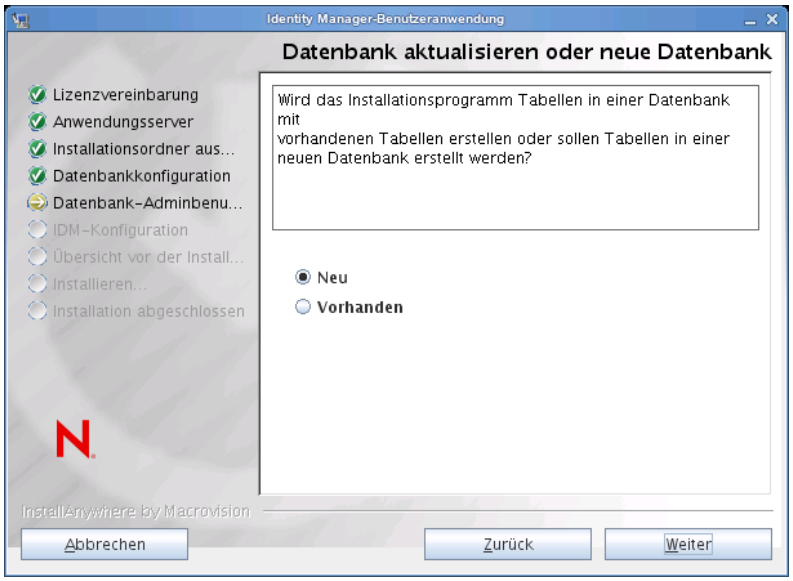
Installationsbildschirm	Beschreibung
Installationstyp	*Rollenbasierte Bereitstellung*: Wählen Sie diese Option aus, um das rollenbasierte Bereitstellungsmodul zu installieren. In dieser Version wird nur diese Installationsart unterstützt.
Installationsordner auswählen	Geben Sie an, wo das Installationsprogramm die Dateien speichern soll.
Datenbankplattform	Wählen Sie die Datenbankplattform. Die Datenbank- und JDBC-Treiber müssen bereits installiert sein. Für WebSphere gibt es folgende Optionen: ◆ Oracle ◆ Microsoft SQL Server ◆ IBM DB2 ◆ PostgreSQL

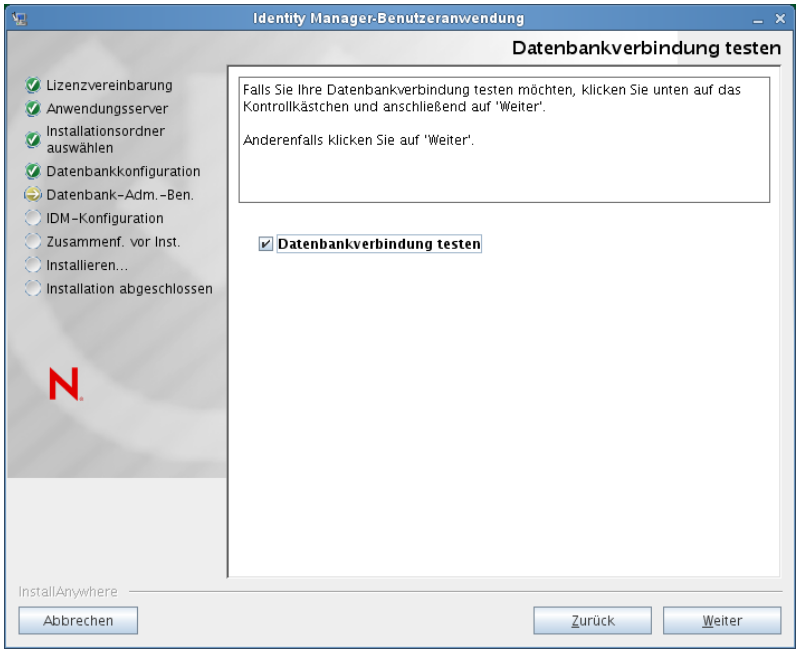
Installationsbildschirm	Beschreibung
Datenbank-Host und Port	*Host*: Geben Sie den Hostnamen oder die IP-Adresse des Datenbankservers an. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied derselbe Hostname bzw. dieselbe IP-Adresse angegeben werden. *Port*: Geben Sie die Listener-Portnummer der Datenbank an. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied derselbe Port angegeben werden. 

Installationsbildschirm	Beschreibung

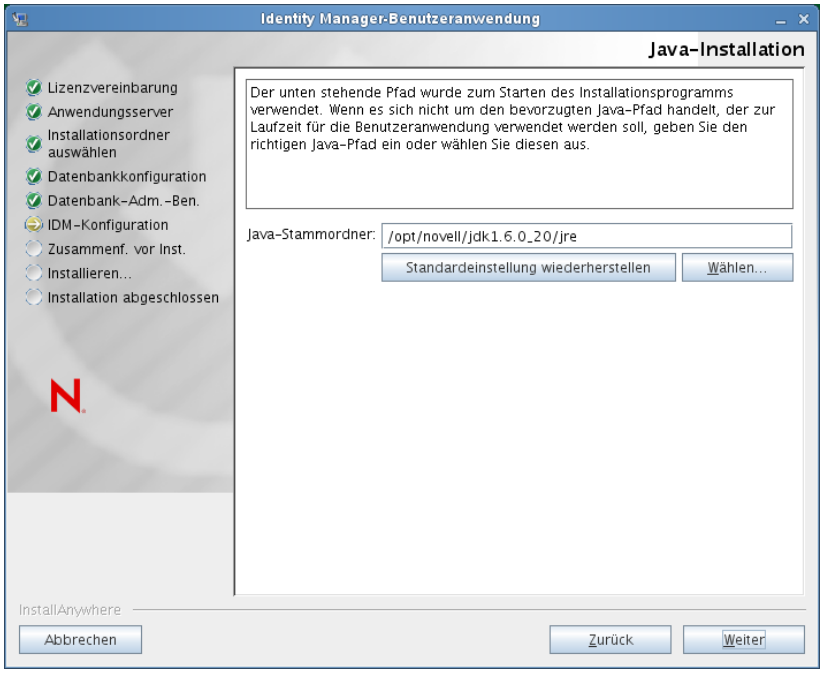
Datenbankbenutzername und Passwort	*Datenbankname* (oder SID): Geben Sie für DB2, MS SQL Server oder PostgreSQL den Namen Ihrer vorkonfigurierten Datenbank an. Geben Sie für Oracle den zuvor erstellten Oracle System Identifier (SID) ein. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied derselbe Datenbankname bzw. derselbe SID angegeben werden.
	
	*Datenbankbenutzer*name: Geben Sie den Datenbankbenutzer an. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied dieselbe Datenbank angegeben werden.
	
	Datenbankpasswort: Geben Sie das Datenbankpasswort an. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied dasselbe Passwort angegeben werden.
	
	Datenbanktreiber-JAR-Datei Geben Sie die Thin-Client-JAR-Datei für den Datenbankserver an. Dieser ist erforderlich.
	
	Wichtig: Mithilfe der Schaltfläche „Durchsuchen“ des Felds *Datenbanktreiber-JAR-Datei* können Sie nur eine (1) JAR-Datei auswählen. Sie müssen aber für DB2 zwei (2) JAR-Dateien angeben:
	◆ db2jcc.jar
	◆ db2jcc_license_cu.jar
	
	Sie können also eine JAR-Datei auswählen. Die zweite Datei müssen Sie allerdings manuell eingeben und dabei das richtige Dateitrennzeichen für das Betriebssystem verwenden, auf dem das Installationsprogramm ausgeführt wird. Alternativ können Sie beide Dateinamen manuell eingeben.
	
	Zum Beispiel unter Windows:
	
	`c:\db2jars\db2jcc.jar;c:\db2jars\db2jcc_license_cu.jar`
	
	Beispielsweise unter Solaris und Linux:
	
	`/home/lab/db2jars/db2jcc.jar:/home/lab/db2jcc_license_cu.jar`
	
	 

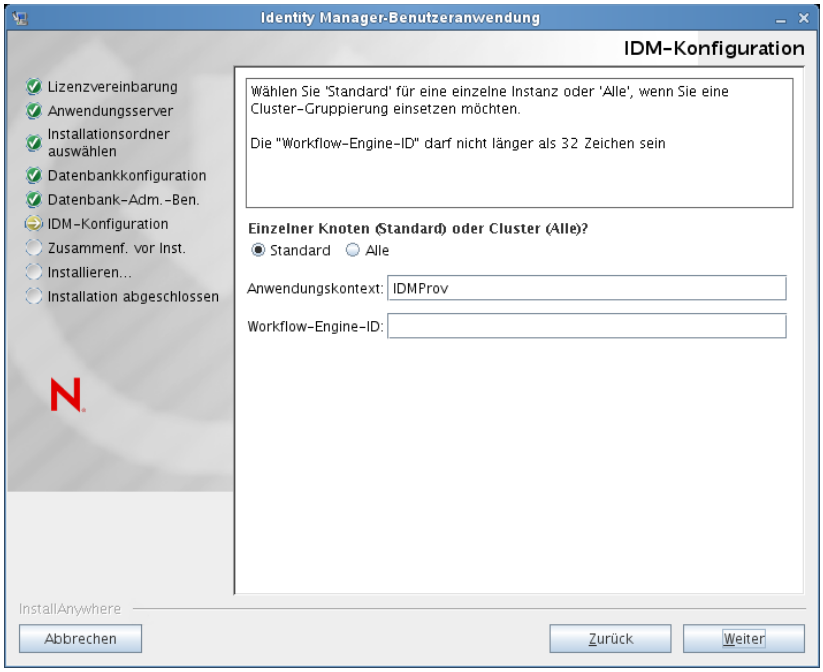
Installationsbildschirm	Beschreibung
Datenbankadministrator	Dieser Bildschirm ist bereits mit dem auf der Seite „Datenbankbenutzername und Passwort“ angegebenen Benutzernamen und Passwort ausgefüllt. Falls der angegebene Datenbankbenutzer nicht über die erforderlichen Berechtigungen zum Erstellen von Tabellen auf dem Datenbankserver verfügt, muss eine andere Benutzer-ID mit den erforderlichen Rechten eingegeben werden. 
Datenbanktabellen erstellen	Geben Sie an, wann die Datenbanktabellen erstellt werden sollen: 

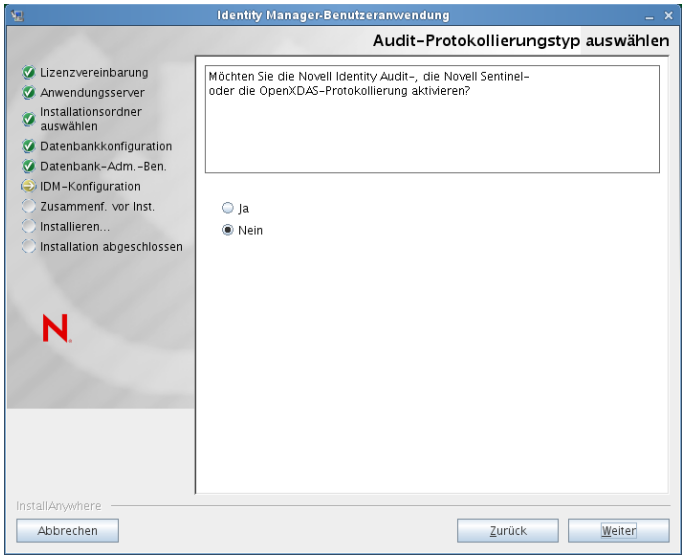
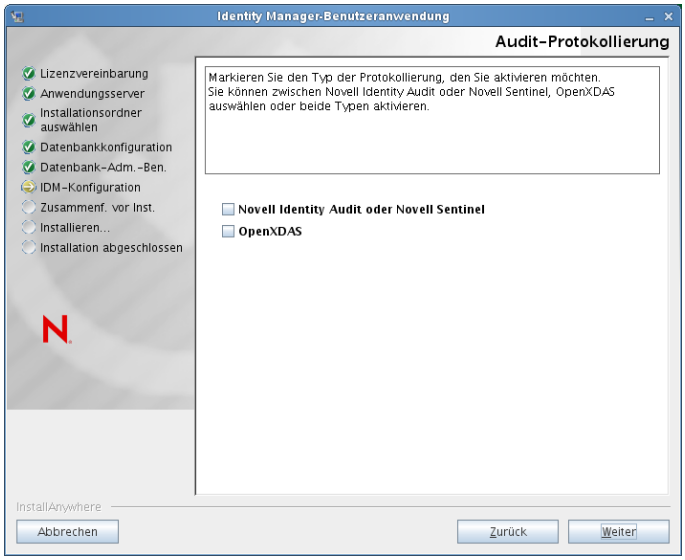
Installationsbildschirm	Beschreibung
Neue Datenbank oder vorhandene Datenbank	Falls die zu verwendende Datenbank neu oder leer ist, klicken Sie auf *Neue Datenbank*. Wenn es sich bei der Datenbank um eine Datenbank einer vorherigen Installation handelt, klicken Sie auf *Vorhandene Datenbank*. 

Installationsbildschirm	Beschreibung
Datenbankverbindung testen	Sie können zum Sicherstellen, dass die Informationen in den vorherigen Bildschirmen korrekt sind, die Datenbankverbindung testen, indem Sie das Kontrollkästchen *Datenbankverbindung testen* aktivieren:  Das Installationsprogramm muss sowohl zum direkten Erstellen von Tabellen als auch zum Erstellen der .SQL-Datei eine Verbindung zur Datenbank herstellen. Wenn Sie die Datenbankverbindung testen und der Test fehlschlägt, können Sie dennoch mit der Installation fortfahren. In diesem Fall müssen Sie die Tabellen nach der Installation erstellen, wie im *Benutzeranwendung: Administrationshandbuch* (http://www.novell.com/documentation/idm40/agpro/?page=/documentation/idm40/agpro/data/bncf7rj.html) beschrieben.

6 Verwenden Sie die nachfolgenden Informationen, um Java und IDM sowie die Audit-Einstellungen und die Sicherheit zu konfigurieren.

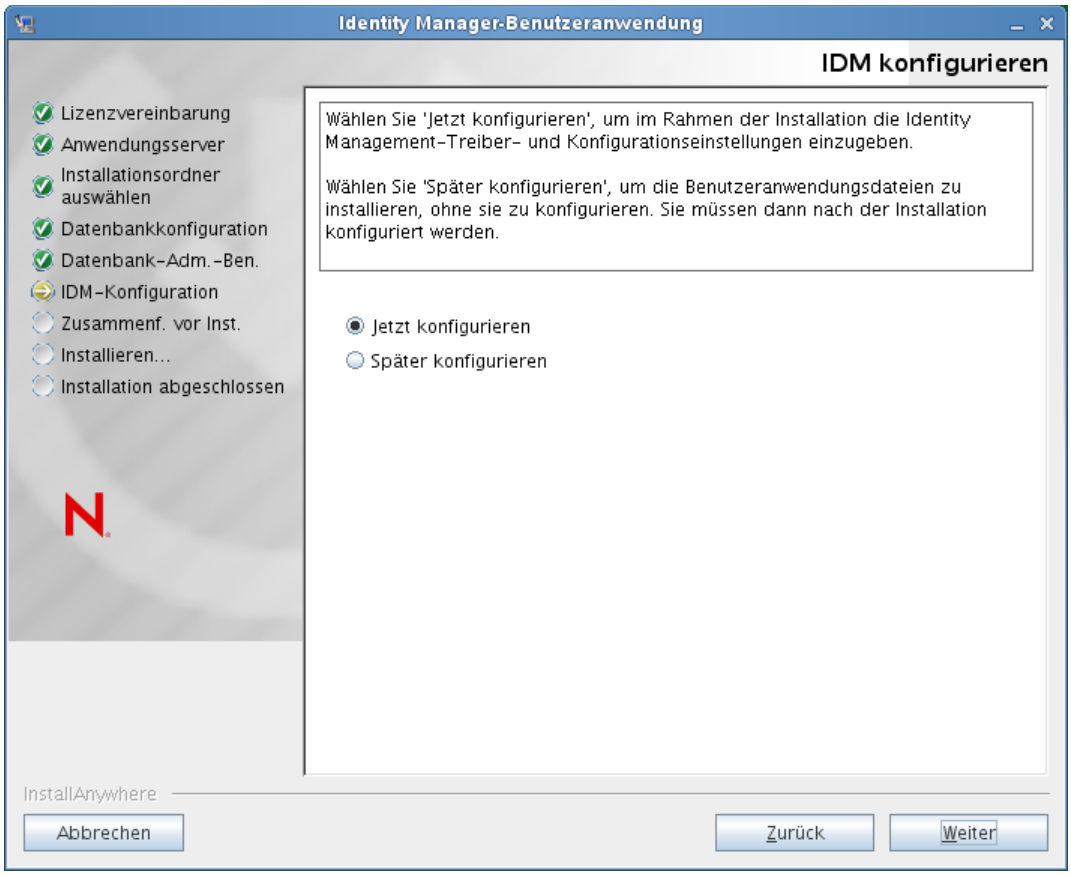
Installationsbildschirm	Beschreibung
Java-Installation	Geben Sie den Java-Stamminstallationsordner an. Die Java-Installation gibt anhand des Werts der Umgebungsvariablen „JAVA_HOME“ den Java-Pfad an und bietet Ihnen die Möglichkeit, den Pfad ggf. zu korrigieren:  Zu diesem Zeitpunkt überprüft das Installationsprogramm, ob die ausgewählte Java-Umgebung für den ausgewählten Anwendungsserver korrekt ist. Zudem wird überprüft, ob das Installationsprogramm in die cacerts-Datei der angegebenen JRE schreiben kann.

Installationsbildschirm	Beschreibung
IDM-Konfiguration	Wählen Sie den Anwendungsserver-Konfigurationstyp: ◆ Wählen Sie *Standard*, wenn diese Installation für einen einzelnen Knoten erfolgt, der nicht Teil eines Clusters ist. Wenn Sie *Standard* auswählen und zu einem späteren Zeitpunkt einen Cluster benötigen, müssen Sie die Benutzeranwendung erneut installieren. ◆ Wählen Sie *Alle*, wenn diese Installation für ein Cluster erfolgt. *Anwendungskontext*: Der Name der Anwendungsserver-Konfiguration, der Name der WAR-Datei der Anwendung und der Name des URL-Kontexts. Das Installations-Skript erstellt eine Serverkonfiguration und benennt die Konfiguration standardmäßig auf der Basis des *Anwendungsnamens*. Notieren Sie den Anwendungsnamen und fügen Sie ihn in die URL ein, wenn Sie die Benutzeranwendung über einen Browser starten. 

Installationsbildschirm	Beschreibung
Audit-Protokollierungstyp auswählen	Klicken Sie auf *Ja*, um die Protokollierung zu aktivieren. Klicken Sie auf *Nein*, um die Protokollierung zu deaktivieren.  Im nächsten Teilfenster werden Sie aufgefordert, den Typ für die Protokollierung anzugeben. Treffen Sie eine Auswahl aus den folgenden Optionen: ◆ *Novell Identity Audit oder Novell Sentinel*: Ermöglicht die Protokollierung über einen Novell-Client für die Benutzeranwendung. ◆ *OpenXDAS*: Ereignisse werden auf Ihrem OpenXDAS-Protokollierungsserver protokolliert. Weitere Informationen zum Einrichten der Protokollierung finden Sie im *Benutzeranwendung: Administrationshandbuch*. 

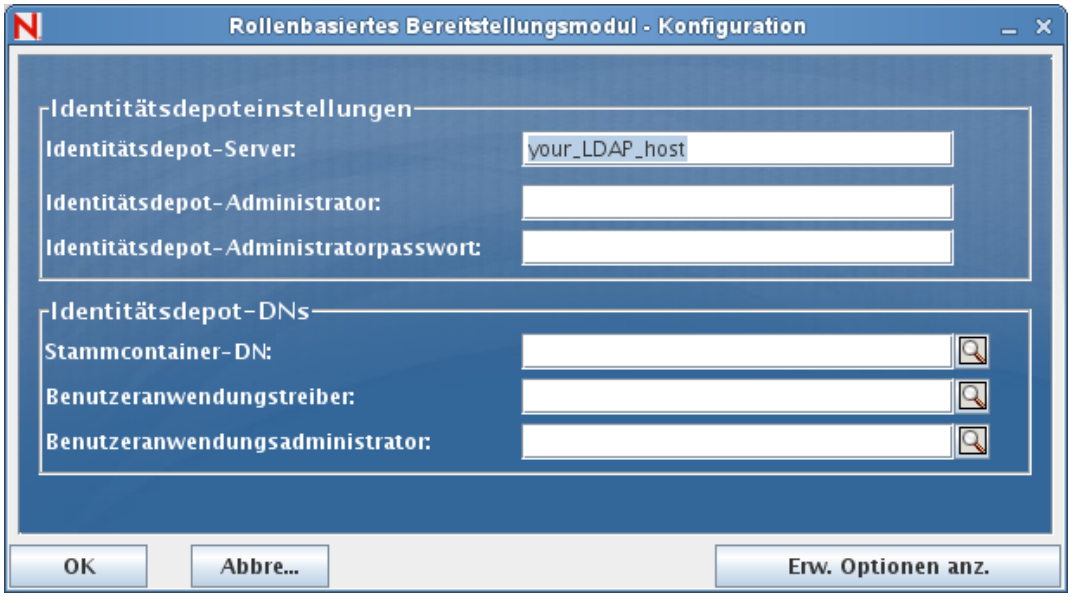
Installationsbildschirm	Beschreibung
Novell Identity Audit oder Novell Sentinel	*Server*: Geben Sie den Hostnamen oder die IP-Adresse des Servers an, sofern Sie die Protokollierung aktivieren. Wenn Sie die Protokollierung deaktivieren, wird dieser Wert ignoriert. *Ordner für Cache-Protokoll*: Geben Sie das Verzeichnis für den Protokollierungs-Cache-Speicher an.
Sicherheit - Master-Schlüssel	*Ja*: Erlaubt den Import eines vorhandenen Master-Schlüssels. Wenn ein vorhandener verschlüsselter Master-Schlüssel importiert werden soll, kopieren Sie den Schlüssel und fügen Sie ihn in das Fenster des Installationsvorgangs ein. *Nein*: Erstellt einen neuen Master-Schlüssel. Nach Abschluss der Installation müssen Sie den Master-Schlüssel manuell speichern, wie in Abschnitt 9.1, „Aufzeichnen des Master-Schlüssels“, auf Seite 149 beschrieben. Bei der Installation wird der verschlüsselte Master-Schlüssel im Installationsverzeichnis in die Datei `master-key.txt` geschrieben. Mögliche Gründe für den Import eines vorhandenen Master-Schlüssels: ◆ Sie verlagern Ihre Installation aus einem Staging-System in ein Produktionssystem und möchten auch weiterhin auf die Datenbank des Staging-Systems zugreifen. ◆ Sie haben die Benutzeranwendung als erstes Mitglied eines Clusters installiert und führen nun die Installation auf nachfolgenden Cluster-Mitgliedern durch (für die derselbe Master-Schlüssel benötigt wird). ◆ Bedingt durch einen Festplattenfehler müssen Sie die Benutzeranwendung wiederherstellen. Sie müssen die Benutzeranwendung neu installieren und den Master-Schlüssel der vorherigen Installation angeben. Auf diese Weise erhalten Sie Zugriff auf zuvor gespeicherte verschlüsselte Daten.

7 Wenn Sie RBPM jetzt konfigurieren möchten, wählen Sie *Jetzt konfigurieren* aus und klicken Sie auf *Weiter*.



(Wenn Sie nicht zur Eingabe dieser Informationen aufgefordert werden, haben Sie möglicherweise die in Abschnitt 2.5, „Installieren des Java Development Kit“, auf Seite 32 aufgeführten Schritte nicht ausgeführt.)

Die Standardansicht des Konfigurationsfensters für das rollenbasierte Bereitstellungsmodul enthält diese sechs Felder:



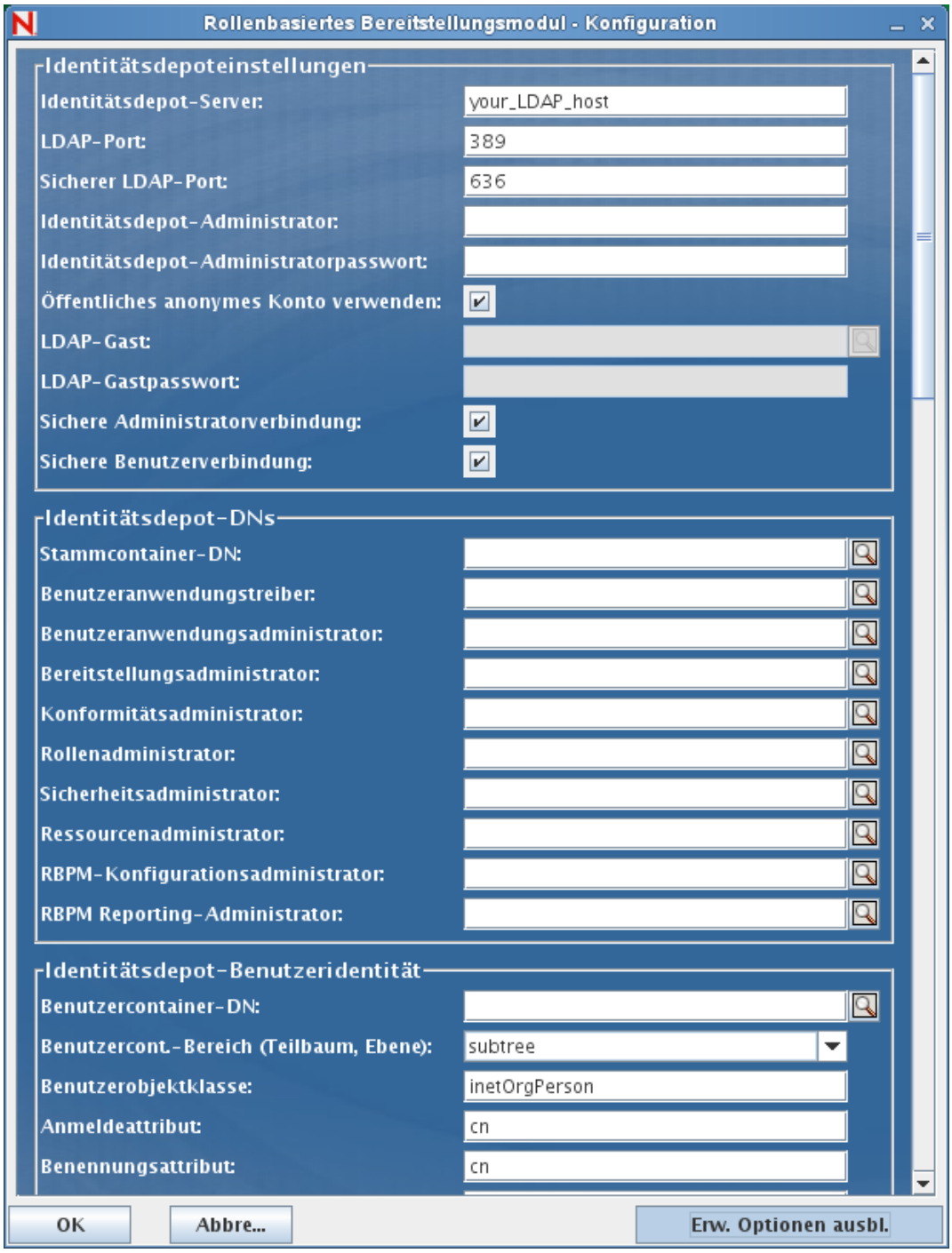
Das Installationsprogramm übernimmt den Wert aus der Stammcontainer-DN und wendet ihn auf die folgenden Werte an:

- Benutzercontainer-DN
- Gruppencontainer-DN

Das Installationsprogramm übernimmt den Wert aus den Benutzeranwendungsadministratorfeldern und wendet ihn auf die folgenden Werte an:

- Bereitstellungsadministrator
- Konformitätsadministrator
- Rollenadministrator
- Sicherheitsadministrator
- Ressourcenadministrator
- RBPM-Konfigurationsadministrator

Wenn Sie diese Werte explizit angeben möchten, klicken Sie auf *Erweiterte Optionen anzeigen* und ändern Sie sie:



Bei der Installation der Benutzeranwendung können Sie Konfigurationsparameter für die Benutzeranwendung festlegen. Die meisten dieser Parameter können auch nach der Installation in der Datei `configupdate.sh` oder `configupdate.bat` bearbeitet werden. Auf Ausnahmen wird in den Parameterbeschreibungen hingewiesen.

Unter Anhang A, „IDM Benutzeranwendung - Konfigurationsreferenz“, auf Seite 157 finden Sie eine Beschreibung für jede Option.

8 Mithilfe der folgenden Informationen wird die Installation ausgeführt.

Installationsbildschirm	Beschreibung
Zusammenfassung vor der Installation	Überprüfen Sie auf der Seite „Zusammenfassung vor der Installation“ die Einstellungen der Installationsparameter. Wenn Sie Änderungen vornehmen möchten, können Sie über die Schaltfläche *Zurück* vorherige Installationsseiten aufrufen. Die Werte auf der Seite „Benutzeranwendung - Konfiguration“ werden nicht gespeichert, daher müssen Sie die Einstellungen auf dieser Seite erneut vornehmen, wenn Sie vorherige Seiten des Installationsvorgangs ändern. Wenn Sie die gewünschten Änderungen an den Installations- und Konfigurationsparametern vorgenommen haben, kehren Sie zur Seite „Zusammenfassung vor der Installation“ zurück und klicken Sie auf *Installieren*.
Installation abgeschlossen	Zeigt an, dass die Installation abgeschlossen ist.

6.1.1 Anzeigen der Installationsprotokolldateien

Wenn die Installation ohne Fehler abgeschlossen wurde, fahren Sie mit Abschnitt 6.2.2, „Hinzufügen von Benutzeranwendungs-Konfigurationsdateien und JVM-Systemeigenschaften“, auf Seite 104 fort.

Sofern bei der Installation Fehler- oder Warnmeldungen ausgegeben wurden, ermitteln Sie die Probleme anhand der Protokolldateien:

- Die Datei `Identity_Manager_User_Application_InstallLog.log` enthält die Ergebnisse der wichtigsten Installationsaufgaben.
- Die Datei `Novell-Custom-Install.log` enthält Informationen zur Konfiguration der Benutzeranwendung, die während der Installation vorgenommen wurde.

6.2 Konfigurieren der WebSphere-Umgebung

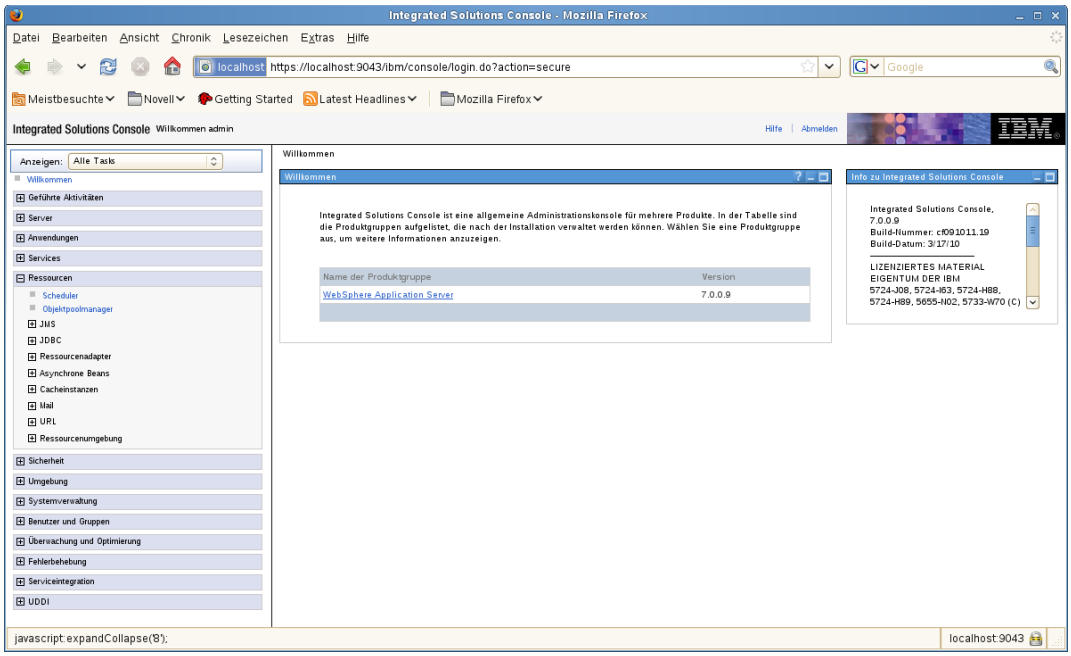
- Abschnitt 6.2.1, „Konfiguration eines Verbindungspools“, auf Seite 96
- Abschnitt 6.2.2, „Hinzufügen von Benutzeranwendungs-Konfigurationsdateien und JVM-Systemeigenschaften“, auf Seite 104
- Abschnitt 6.2.3, „Importieren der eDirectory-Herkunftsverbürgung in den WebSphere-Keystore“, auf Seite 110
- Abschnitt 6.2.4, „Übergeben der preferIPv4Stack-Eigenschaft an die JVM“, auf Seite 111

6.2.1 Konfiguration eines Verbindungspools

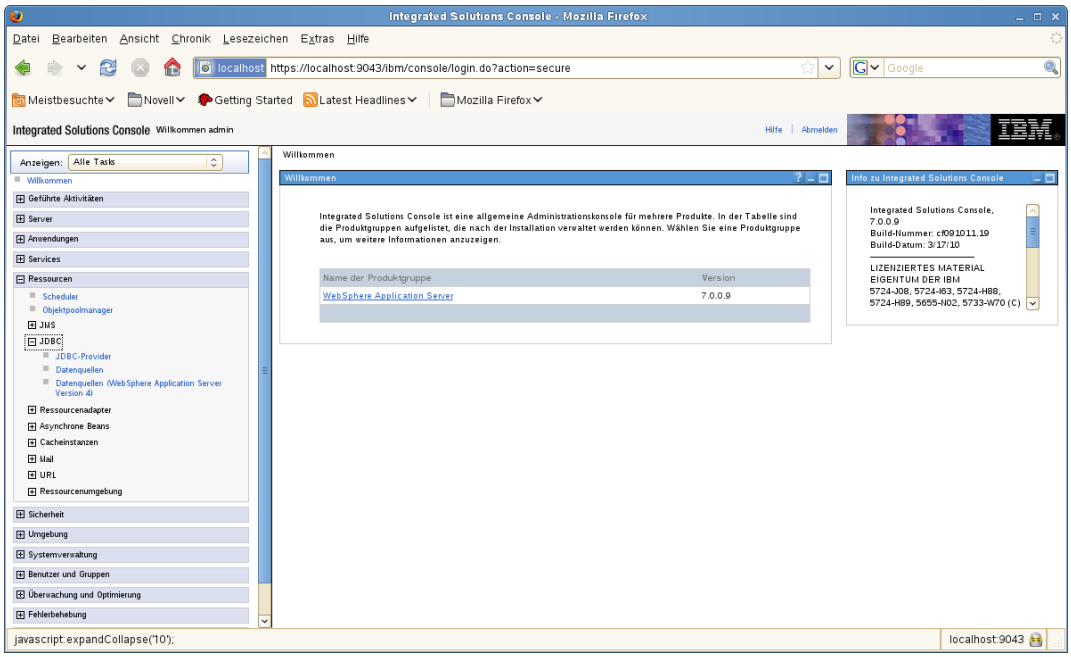
Zum Konfigurieren eines Verbindungspools zur Verwendung mit WebSphere müssen Sie einen JDBC-Provider und eine Datenquelle erstellen. Dieser Abschnitt enthält Anweisungen zum Erstellen des Providers und der Datenquelle.

So erstellen Sie einen JDBC-Provider:

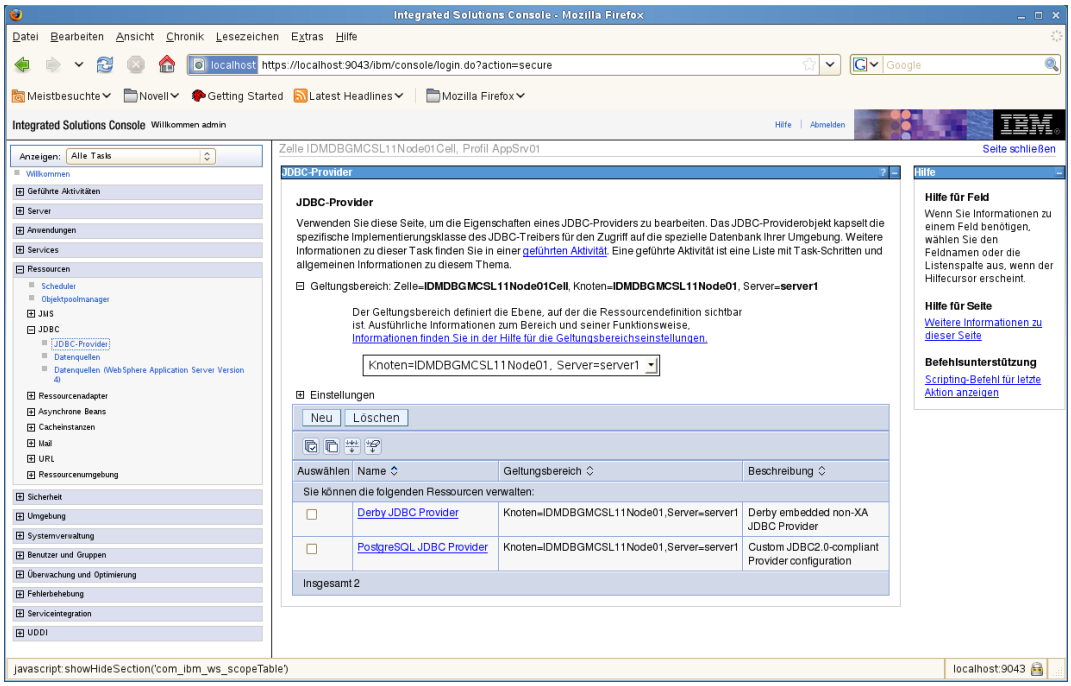
1 Erweitern Sie *Resources* links auf der Seite „Integrated Solutions Console“:



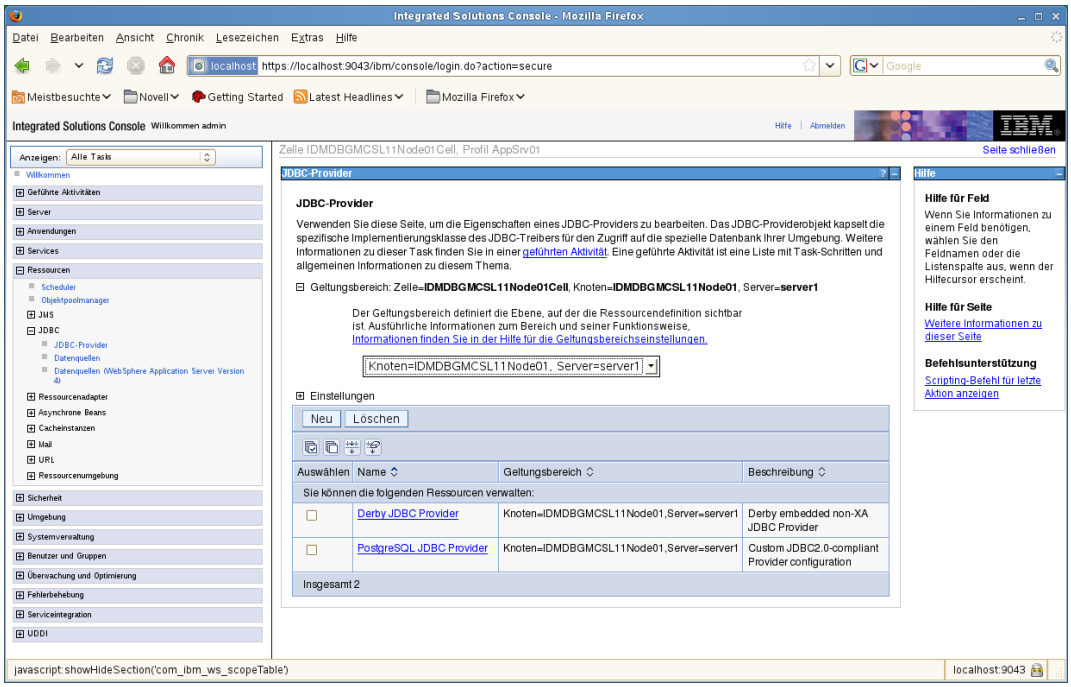
2 Erweitern Sie *JDBC*:



3 Klicken Sie auf *JDBC-Provider*:


Integrated Solutions Console - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
https://localhost:9043/ibm/console/login.do?action=secure
Integrated Solutions Console Willkommen admin
Zelle IDMDBGMCSL11Node01Cell, Profil AppSrv01
Seite schließen
JDBC-Provider
JDBC-Provider
Verwenden Sie diese Seite, um die Eigenschaften eines JDBC-Providers zu bearbeiten. Das JDBC-Providerobjekt kapselt die spezifische Implementierungsklasse des JDBC-Treibers für den Zugriff auf die spezielle Datenbank Ihrer Umgebung. Weitere Informationen zu dieser Task finden Sie in einer geführten Aktivität. Eine geführte Aktivität ist eine Liste mit Task-Schritten und allgemeinen Informationen zu diesem Thema.
Geltungsbereich: Zelle=IDMDBGMCSL11Node01Cell, Knoten=IDMDBGMCSL11Node01, Server=server1
Der Geltungsbereich definiert die Ebene, auf der die Ressourcendefinition sichtbar ist. Ausführliche Informationen zum Bereich und seiner Funktionsweise, Informationen finden Sie in der Hilfe für die Geltungsbereichseinstellungen.
Knoten=IDMDBGMCSL11Node01, Server=server1
Einstellungen
Neu
Löschen
Auswählen
Name
Geltungsbereich
Beschreibung
Sie können die folgenden Ressourcen verwalten:
Derby JDBC Provider
Knoten=IDMDBGMCSL11Node01,Server=server1
Derby embedded non-XA JDBC Provider
PostgreSQL JDBC Provider
Knoten=IDMDBGMCSL11Node01,Server=server1
Custom JDBC2.0-compliant Provider configuration
Insgesamt 2
Hilfe
Hilfe für Feld
Wenn Sie Informationen zu einem Feld benötigen, wählen Sie den Feldnamen oder die Listenspalte aus, wenn der Hilfecursor erscheint.
Hilfe für Seite
Weitere Informationen zu dieser Seite
Befehlsunterstützung
Scripting-Befehl für letzte Aktion anzeigen
javascript:showHideSection('com_ibm_ws_scopeTable')
localhost:9043

4 Erweitern Sie *Geltungsbereich*:

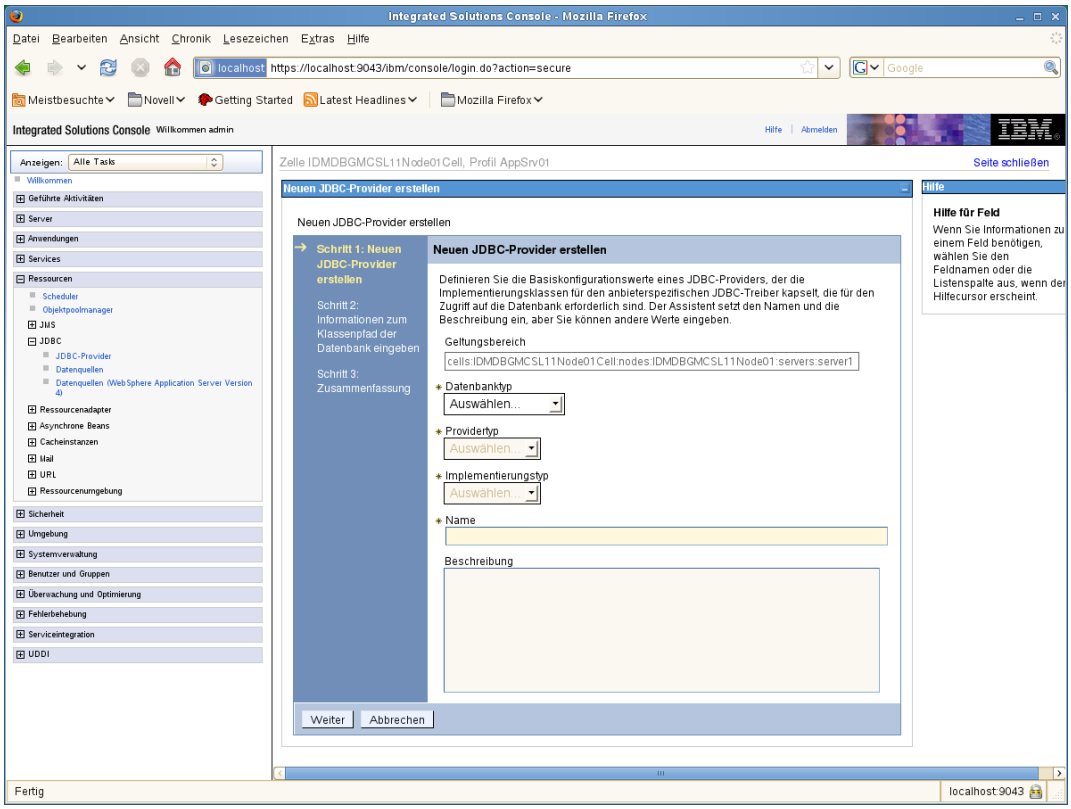

Integrated Solutions Console - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
https://localhost:9043/ibm/console/login.do?action=secure
Integrated Solutions Console Willkommen admin
Zelle IDMDBGMCSL11Node01Cell, Profil AppSrv01
Seite schließen
JDBC-Provider
JDBC-Provider
Verwenden Sie diese Seite, um die Eigenschaften eines JDBC-Providers zu bearbeiten. Das JDBC-Providerobjekt kapselt die spezifische Implementierungsklasse des JDBC-Treibers für den Zugriff auf die spezielle Datenbank Ihrer Umgebung. Weitere Informationen zu dieser Task finden Sie in einer geführten Aktivität. Eine geführte Aktivität ist eine Liste mit Task-Schritten und allgemeinen Informationen zu diesem Thema.
Geltungsbereich: Zelle=IDMDBGMCSL11Node01Cell, Knoten=IDMDBGMCSL11Node01, Server=server1
Der Geltungsbereich definiert die Ebene, auf der die Ressourcendefinition sichtbar ist. Ausführliche Informationen zum Bereich und seiner Funktionsweise, Informationen finden Sie in der Hilfe für die Geltungsbereichseinstellungen.
Knoten=IDMDBGMCSL11Node01, Server=server1
Einstellungen
Neu
Löschen
Auswählen
Name
Geltungsbereich
Beschreibung
Sie können die folgenden Ressourcen verwalten:
Derby JDBC Provider
Knoten=IDMDBGMCSL11Node01,Server=server1
Derby embedded non-XA JDBC Provider
PostgreSQL JDBC Provider
Knoten=IDMDBGMCSL11Node01,Server=server1
Custom JDBC2.0-compliant Provider configuration
Insgesamt 2
Hilfe
Hilfe für Feld
Wenn Sie Informationen zu einem Feld benötigen, wählen Sie den Feldnamen oder die Listenspalte aus, wenn der Hilfecursor erscheint.
Hilfe für Seite
Weitere Informationen zu dieser Seite
Befehlsunterstützung
Scripting-Befehl für letzte Aktion anzeigen
javascript:showHideSection('com_ibm_ws_scopeTable')
localhost:9043

5 Wählen Sie *Knoten=IhrServername, Server=server1*.

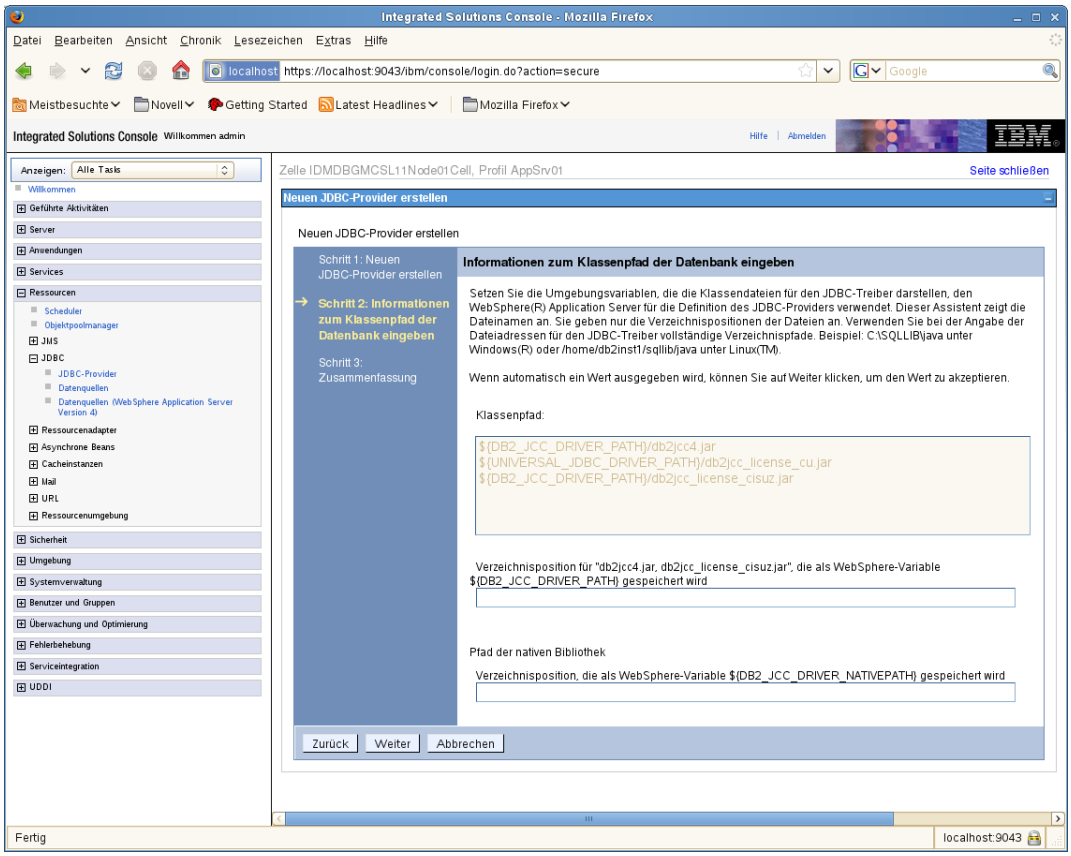
6 Klicken Sie auf die Schaltfläche *Neu*.

7 Wählen Sie den *Datenbanktyp* aus (z. B. DB2).

8 Klicken Sie auf *Weiter*.



9 Geben Sie die JDBC-Klassenpfadinformationen ein.



10 Klicken Sie auf *Weiter*.

11 Klicken Sie auf *Fertig stellen*.

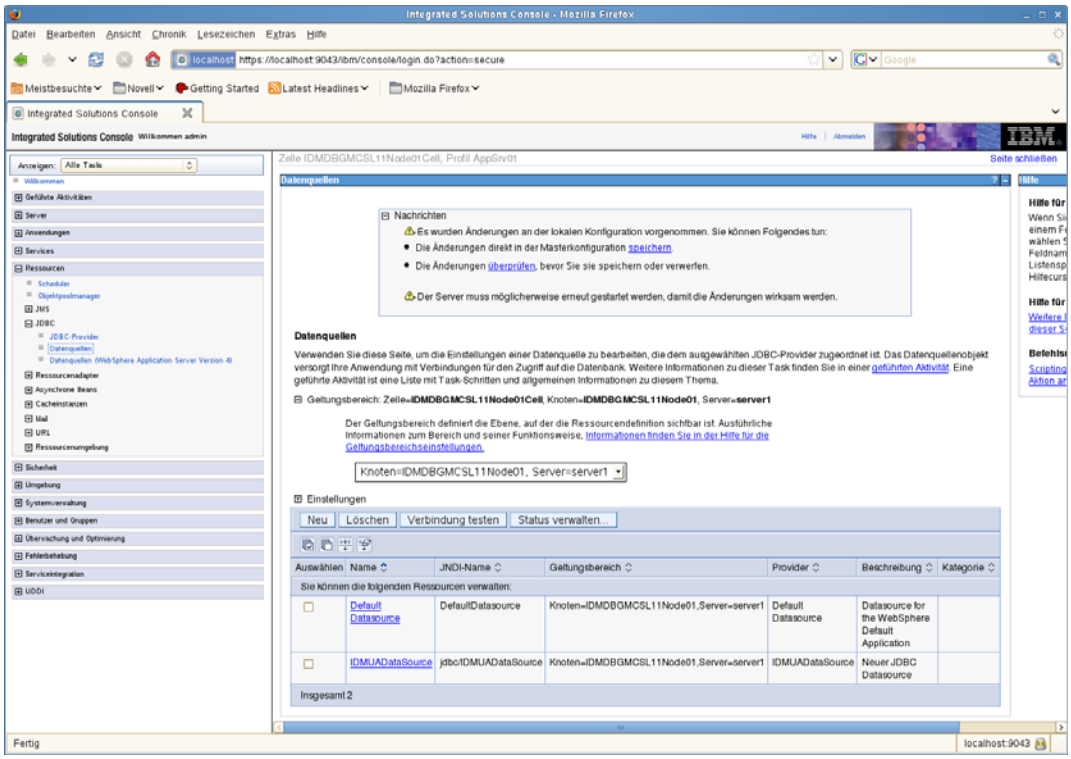
12 Klicken Sie auf den Link *Speichern*.

So erstellen Sie eine Datenquelle:

1 Erweitern Sie *Ressourcen* im linken Seitenbereich.

2 Erweitern Sie *JDBC*.

3 Klicken Sie auf *Datenquellen*.


Integrated Solutions Console - Mozilla Firefox
Integrated Solutions Console
Datenquellen
Nachrichten
Es wurden Änderungen an der lokalen Konfiguration vorgenommen. Sie können Folgendes tun:
Die Änderungen direkt in der Masterkonfiguration speichern.
Die Änderungen überprüfen, bevor Sie sie speichern oder verwerfen.
Der Server muss möglicherweise erneut gestartet werden, damit die Änderungen wirksam werden.
Datenquellen
Verwenden Sie diese Seite, um die Einstellungen einer Datenquelle zu bearbeiten, die dem ausgewählten JDBC-Provider zugeordnet ist. Das Datenquellenobjekt versorgt Ihre Anwendung mit Verbindungen für den Zugriff auf die Datenbank. Weitere Informationen zu dieser Task finden Sie in einer geführten Aktivität. Eine geführte Aktivität ist eine Liste mit Task-Schritten und allgemeinen Informationen zu diesem Thema.
Geltungsbereich: Zelle=IDMDBGMCSL11Node01Cell, Knoten=IDMDBGMCSL11Node01, Server=server1
Der Geltungsbereich definiert die Ebene, auf der die Ressourcendefinition sichtbar ist. Ausführliche Informationen zum Bereich und seiner Funktionsweise, Informationen finden Sie in der Hilfe für die Geltungsbereichseinstellungen.
Knoten=IDMDBGMCSL11Node01, Server=server1
Einstellungen
Neu
Löschen
Verbindung testen
Status verwalten...
Auswählen
Name
JNDI-Name
Geltungsbereich
Provider
Beschreibung
Kategorie
Sie können die folgenden Ressourcen verwalten:
Default Datasource
DefaultDatasource
Knoten=IDMDBGMCSL11Node01,Server=server1
Default Datasource
Datasource for the WebSphere Default Application
IDMUADataSource
jdbc/IDMUADataSource
Knoten=IDMDBGMCSL11Node01,Server=server1
IDMUADataSource
Neuer JDBC Datasource
Insgesamt 2
Fertig
localhost:9043

4 Erweitern Sie *Geltungsbereich*.

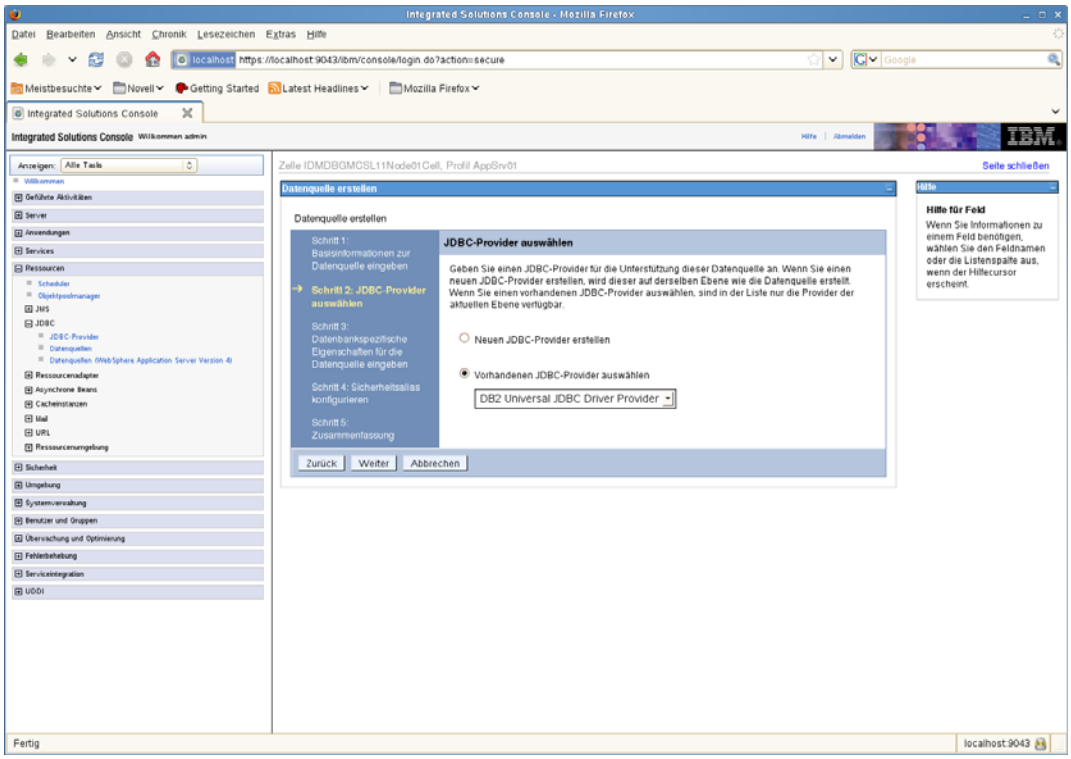
5 Wählen Sie *Knoten=IhrServername, Server=server1*.

6 Klicken Sie auf die Schaltfläche *Neu*.

7 Geben Sie den Namen der Datenquelle und den JNDI-Namen ein (z. B. für beide „IDMUADataSource“).

8 Klicken Sie auf *Weiter*.

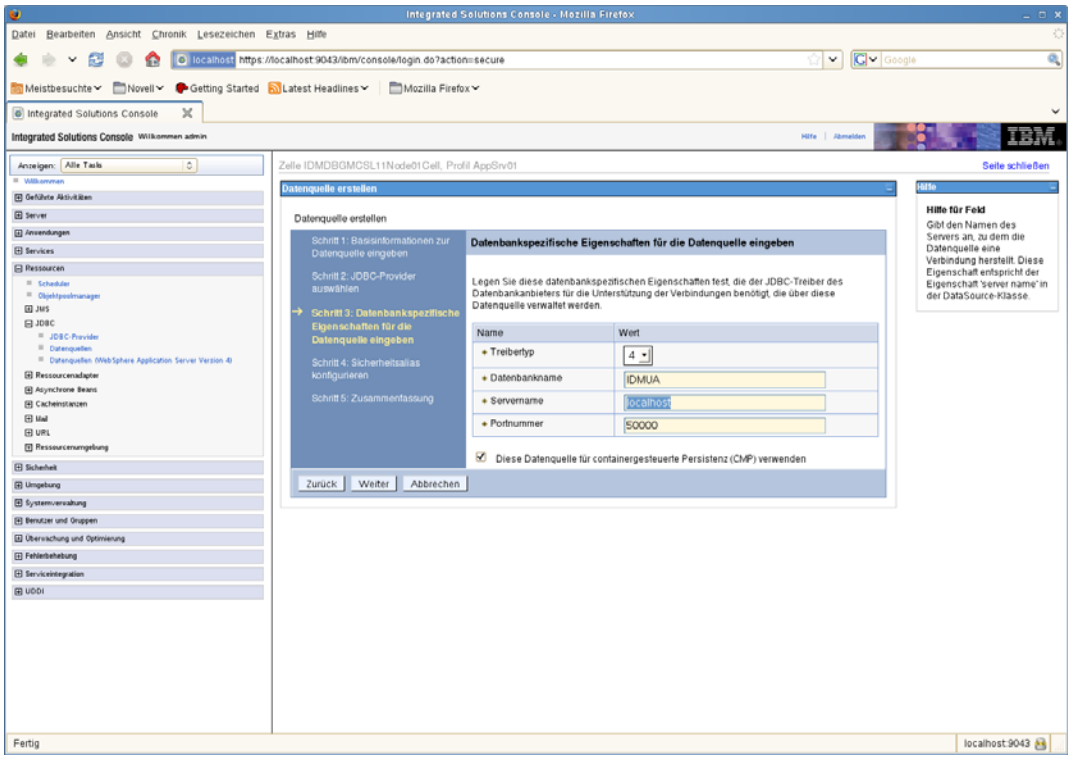
9 Klicken Sie auf *Vorhandenen JDBC-Provider auswählen*.


Integrated Solutions Console - Mozilla Firefox
Integrated Solutions Console
Datenquelle erstellen
Datenquelle erstellen
Schritt 1: Basisinformationen zur Datenquelle eingeben
Schritt 2: JDBC-Provider auswählen
Schritt 3: Datenbankspezifische Eigenschaften für die Datenquelle eingeben
Schritt 4: Sicherheitsalias konfigurieren
Schritt 5: Zusammenfassung
JDBC-Provider auswählen
Geben Sie einen JDBC-Provider für die Unterstützung dieser Datenquelle an. Wenn Sie einen neuen JDBC-Provider erstellen, wird dieser auf derselben Ebene wie die Datenquelle erstellt. Wenn Sie einen vorhandenen JDBC-Provider auswählen, sind in der Liste nur die Provider der aktuellen Ebene verfügbar.
Neuen JDBC-Provider erstellen
Vorhandenen JDBC-Provider auswählen
DB2 Universal JDBC Driver Provider
Zurück
Weiter
Abbrechen
Hilfe für Feld
Fertig
localhost:9043

10 Wählen Sie den zuvor erstellten JDBC-Provider aus.

11 Klicken Sie auf *Weiter*.

12 Geben Sie die erforderlichen Datenbankinformationen für die Datenquelle ein (Datenbankname, Servername, Port, Benutzername und Passwort).



13 Klicken Sie auf *Weiter*.

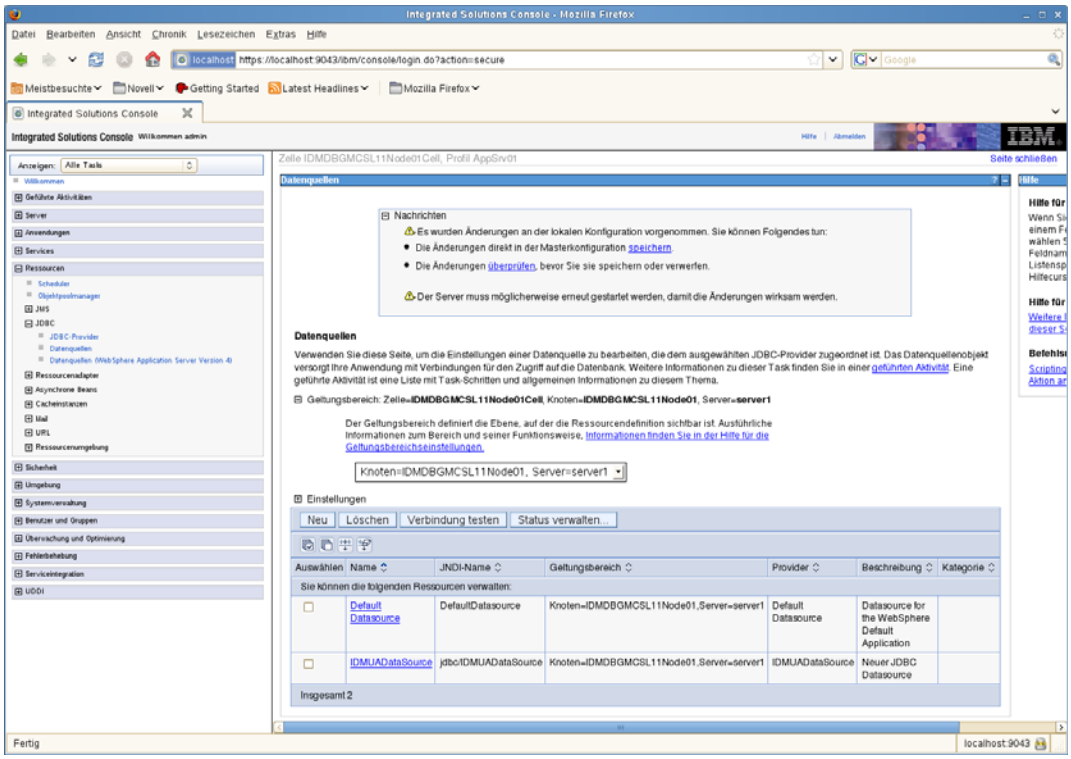
14 Geben Sie Informationen für den Security Alias ein oder behalten Sie die Standardwerte bei.

15 Klicken Sie auf *Weiter*.

16 Klicken Sie auf *Fertig stellen*.

17 Klicken Sie auf *Speichern*.

18 Wählen Sie Ihre neue Datenquelle aus, indem Sie auf das Kontrollkästchen links neben dem Namen klicken.


Integrated Solutions Console - Mozilla Firefox
Integrated Solutions Console
Datenquellen
Nachrichten
Es wurden Änderungen an der lokalen Konfiguration vorgenommen. Sie können Folgendes tun:
Die Änderungen direkt in der Masterkonfiguration speichern.
Die Änderungen überprüfen, bevor Sie sie speichern oder verwerfen.
Der Server muss möglicherweise erneut gestartet werden, damit die Änderungen wirksam werden.
Datenquellen
Verwenden Sie diese Seite, um die Einstellungen einer Datenquelle zu bearbeiten, die dem ausgewählten JDBC-Provider zugeordnet ist. Das Datenquellenobjekt versorgt Ihre Anwendung mit Verbindungen für den Zugriff auf die Datenbank. Weitere Informationen zu dieser Task finden Sie in einer geführten Aktivität. Eine geführte Aktivität ist eine Liste mit Task-Schritten und allgemeinen Informationen zu diesem Thema.
Geltungsbereich: Zelle=IDMDBGMCSL11Node01Cell, Knoten=IDMDBGMCSL11Node01, Server=server1
Der Geltungsbereich definiert die Ebene, auf der die Ressourcendefinition sichtbar ist. Ausführliche Informationen zum Bereich und seiner Funktionsweise, Informationen finden Sie in der Hilfe für die Geltungsbereichseinstellungen.
Knoten=IDMDBGMCSL11Node01, Server=server1
Einstellungen
Neu
Löschen
Verbindung testen
Status verwalten...
Auswählen
Name
JNDI-Name
Geltungsbereich
Provider
Beschreibung
Kategorie
Sie können die folgenden Ressourcen verwalten:
Default Datasource
DefaultDatasource
Knoten=IDMDBGMCSL11Node01,Server=server1
Default Datasource
Datasource for the WebSphere Default Application
IDMUADataSource
jdbc/IDMUADataSource
Knoten=IDMDBGMCSL11Node01,Server=server1
IDMUADataSource
Neuer JDBC Datasource
Insgesamt 2
Fertig
localhost:9043

19 Klicken Sie auf die Schaltfläche *Verbindung testen* und vergewissern Sie sich, dass *Ordnungsgemäß durchgeführt* zurückgegeben wird.

6.2.2 Hinzufügen von Benutzeranwendungs-Konfigurationsdateien und JVM-Systemeigenschaften

Für eine erfolgreiche WebSphere-Installation sind folgende Schritte erforderlich:

1 Kopieren Sie die Datei `sys-configuration-xmldata.xml` aus dem Installationsverzeichnis der Benutzeranwendung in ein Verzeichnis auf dem Computer, der den WebSphere-Server hostet, beispielsweise `/UserAppConfigFiles`.

Das Installationsverzeichnis der Benutzeranwendung ist das Verzeichnis, in dem Sie die Benutzeranwendung installiert haben.

2 Geben Sie den Pfad zur Datei `sys-configuration-xmldata.xml` in den JVM-Systemeigenschaften an. Melden Sie sich dazu als Admin-Benutzer bei der Administrationskonsole von WebSphere an.

3 Rufen Sie in der linken Kontrollleiste *Server* > *Anwendungsserver* auf.

4 Klicken Sie in der Serverliste auf den Servernamen, z. B. „server1“.

5 Rufen Sie in der Liste der Einstellungen auf der rechten Seite unter *Serverinfrastruktur* die Option *Java- und Prozessverwaltung* auf.

6 Erweitern Sie den Link und wählen Sie *Prozessdefinition*.

7 Wählen Sie aus der Liste *Zusätzliche Eigenschaften* die Option *Java Virtual Machine*.

8 Wählen Sie unter der Überschrift *Zusätzliche Eigenschaften* für die JVM-Seite die Option *Benutzerdefinierte Eigenschaften*.

9 Klicken Sie auf *Neu*, um eine neue JVM-Systemeigenschaft hinzuzufügen.

9a Geben Sie als *Namen* `extend.local.config.dir` an.

9b Geben Sie als *Wert* den Namen des Installationsordners (Verzeichnis) ein, den Sie während der Installation angegeben haben.

Das Installationsprogramm hat in diesem Ordner die Datei `sys-configuration-xmldata.xml` erstellt.

9c Geben Sie unter *Beschreibung* eine Beschreibung der Eigenschaft ein, beispielsweise `Pfad zu sys-configuration-xmldata.xml`.

9d Klicken Sie auf *OK*, um die Eigenschaft zu speichern.

10 Klicken Sie auf *Neu*, um eine weitere neue JVM-Systemeigenschaft hinzuzufügen.

10a Geben Sie als *Namen* `idmuserapp.logging.config.dir` an.

10b Geben Sie als *Wert* den Namen des Installationsordners (Verzeichnis) ein, den Sie während der Installation angegeben haben.

10c Geben Sie unter *Beschreibung* eine Beschreibung der Eigenschaft ein, beispielsweise `Pfad zu idmuserapp_logging.xml`.

10d Klicken Sie auf *OK*, um die Eigenschaft zu speichern.

Die Datei `idmuserapp-logging.xml` wird erst dann erstellt, wenn Sie die Änderungen über *Benutzeranwendung* > *Administration* > *Anwendungskonfiguration* > *Protokollierung* permanent gespeichert haben.

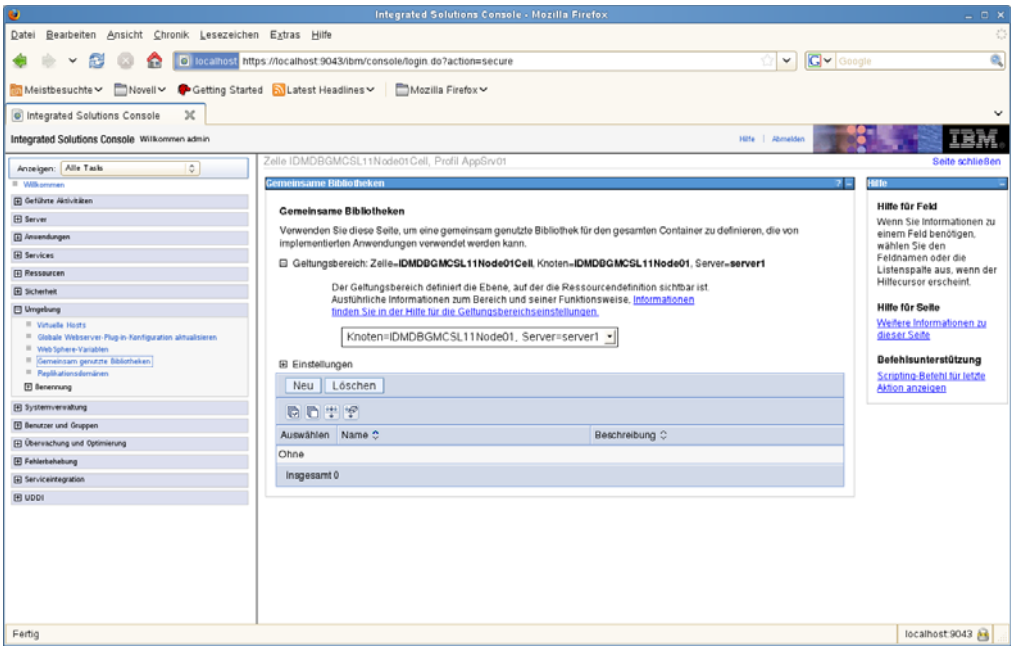
Sie müssen auch eine gemeinsame Bibliothek für die Benutzeranwendung auf WebSphere konfigurieren. Die gemeinsame Bibliothek definiert das Klassenladeverhalten, das erforderlich ist, damit die Anwendung ordnungsgemäß ausgeführt wird.

So konfigurieren Sie die gemeinsame Bibliothek:

1 Erstellen Sie die gemeinsame Bibliothek für die Benutzeranwendung:

1a Klicken Sie im linken Navigationsmenü auf *Umgebung*.

1b Klicken Sie auf *Gemeinsame Bibliotheken*.



1c Klicken Sie auf die Schaltfläche *Neu*.

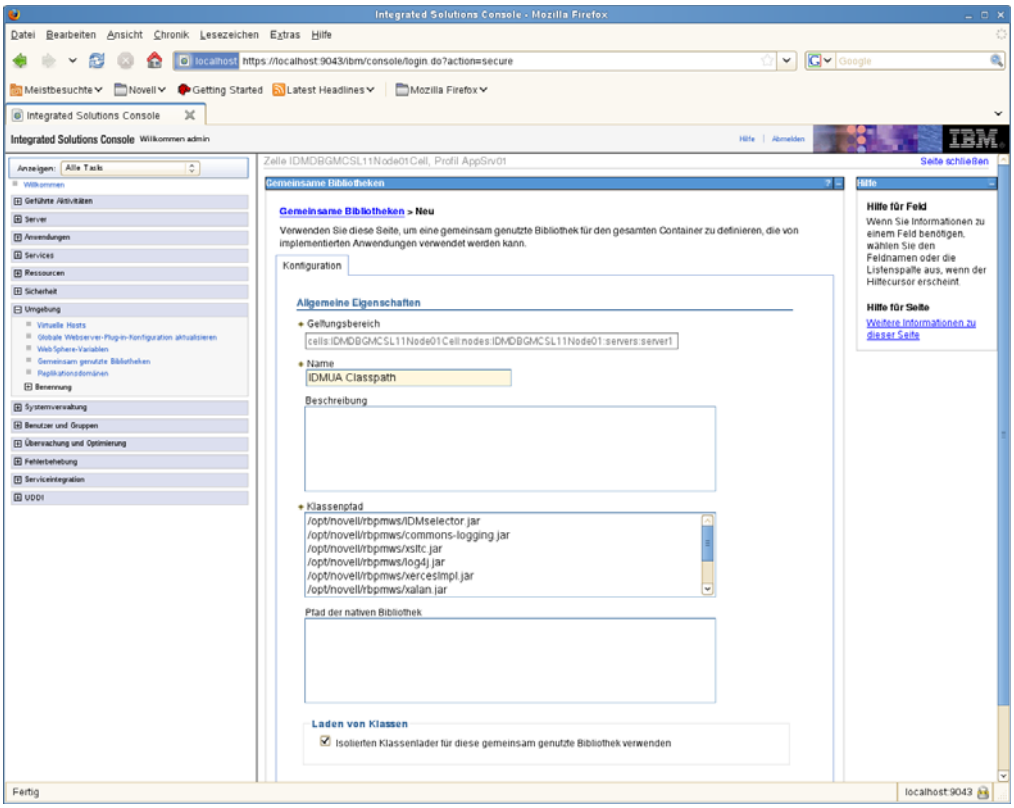
1d Geben Sie einen Namen ein (z. B. „IDMUA Classloader“).

1e Geben Sie die Liste der erforderlichen JAR-Dateien in das Feld „Klassenpfad“ ein:

- `antlr.jar`
- `log4j.jar`
- `commons-logging.jar`

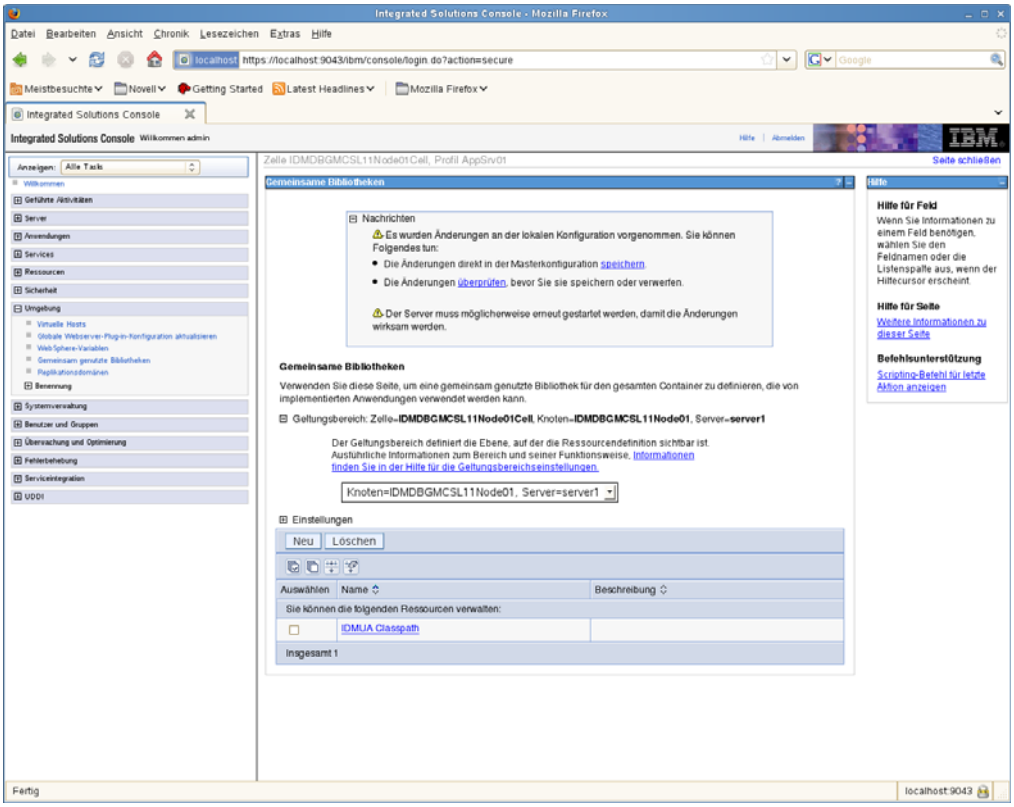
  Hinweis: Sie müssen diese JAR-Datei von der Apache-Website herunterladen.

- `xalan.jar`
- `xercesImpl.jar`
- `xsltc.jar`
- `serializer.jar`
- `jaxb-impl.jar`
- `IDMselector.jar`



1f Klicken Sie auf *OK*.

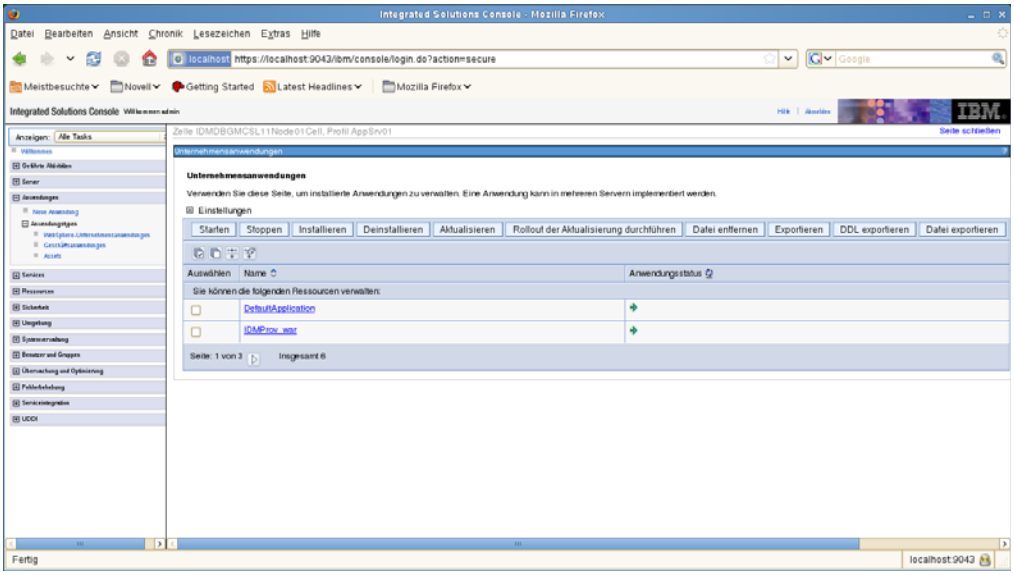
1g Klicken Sie auf den Link *Speichern*.


Integrated Solutions Console - Mozilla Firefox
Integrated Solutions Console
Gemeinsame Bibliotheken
Nachrichten
Es wurden Änderungen an der lokalen Konfiguration vorgenommen. Sie können Folgendes tun:
Die Änderungen direkt in der Masterkonfiguration speichern.
Die Änderungen überprüfen, bevor Sie sie speichern oder verwerfen.
Der Server muss möglicherweise erneut gestartet werden, damit die Änderungen wirksam werden.
Gemeinsame Bibliotheken
Verwenden Sie diese Seite, um eine gemeinsam genutzte Bibliothek für den gesamten Container zu definieren, die von implementierten Anwendungen verwendet werden kann.
Geltungsbereich: Zelle=IDMDBGMCSL11Node01Cell, Knoten=IDMDBGMCSL11Node01, Server=server1
Der Geltungsbereich definiert die Ebene, auf der die Ressourcendefinition sichtbar ist. Ausführliche Informationen zum Bereich und seiner Funktionsweise, Informationen finden Sie in der Hilfe für die Geltungsbereichseinstellungen.
Knoten=IDMDBGMCSL11Node01, Server=server1
Einstellungen
Neu
Löschen
Auswählen
Name
Beschreibung
Sie können die folgenden Ressourcen verwalten:
IDMJA Classpath
Insgesamt 1
Hilfe
Hilfe für Feld
Hilfe für Seite
Befehlsunterstützung
Fertig
localhost:9043

2 Fügen Sie die gemeinsame Bibliothek zu IDMProv hinzu:

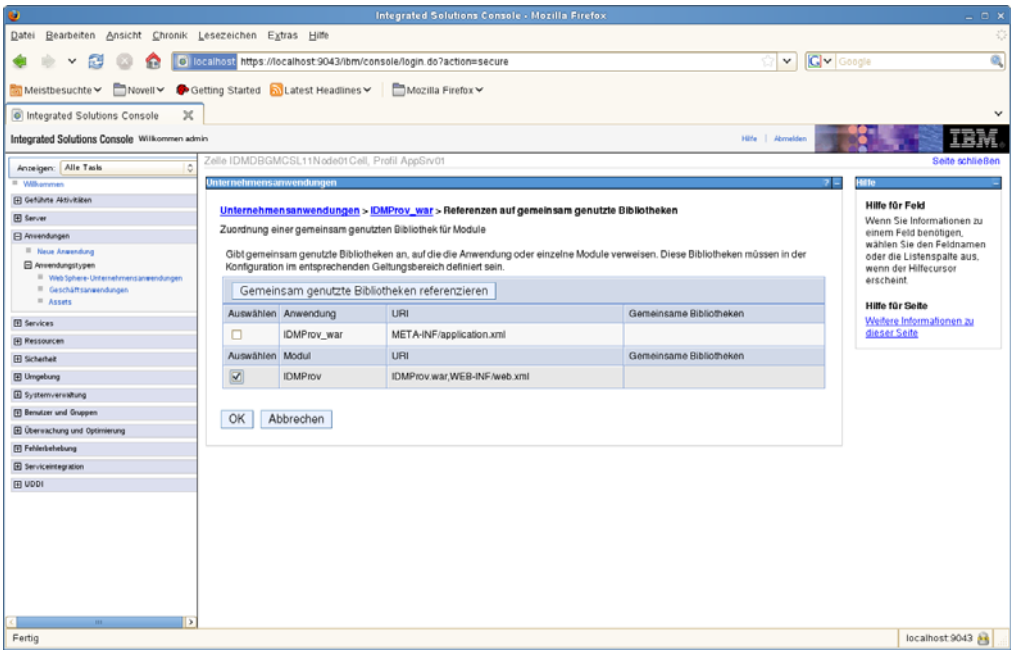
2a Klicken Sie auf der linken Seite auf *Anwendungen*.

2b Klicken Sie auf *WebSphere-Unternehmensanwendungen*.



2c Klicken Sie auf den Namen *IDMProv_war*.

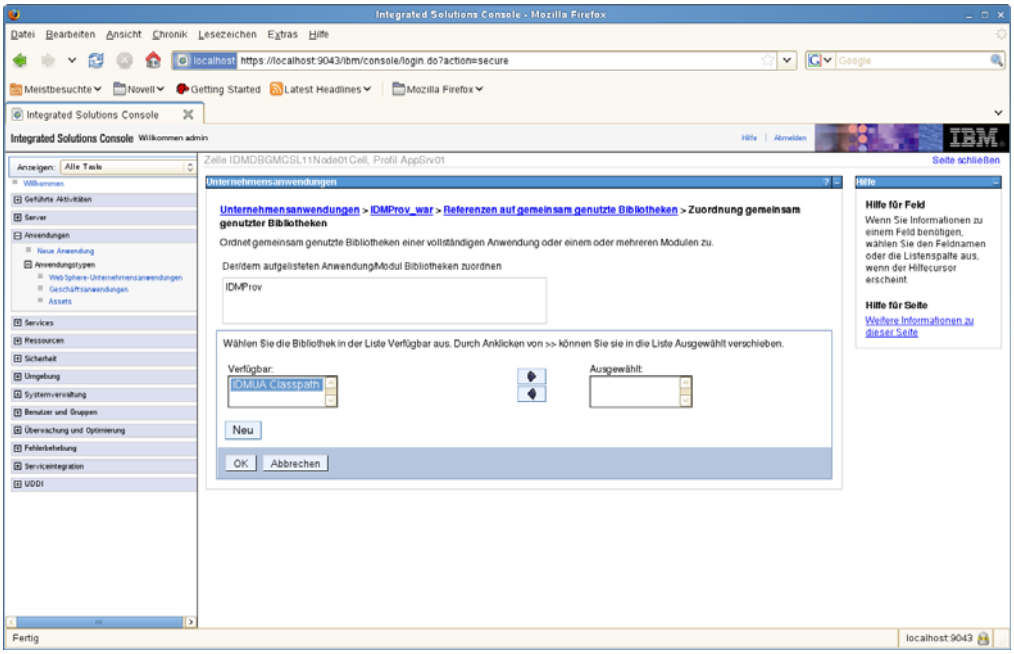
2d Klicken Sie unten auf der Seite unter *Referenzen* auf *Referenzen auf gemeinsam genutzte Bibliotheken*.



2e Klicken Sie auf das Kontrollkästchen neben *IDMProv* (nicht IDMProv_war).

2f Klicken Sie auf die Schaltfläche *Gemeinsam genutzte Bibliotheken referenzieren*.

2g Klicken Sie auf den Namen der gemeinsamen Bibliothek (*IDMUA Classpath*) im Feld *Verfügbar*. Klicken Sie anschließend auf den nach rechts weisenden Pfeil, sodass sie in das Feld *Ausgewählt* verschoben wird.


Integrated Solutions Console - Mozilla Firefox
Integrated Solutions Console
Unternehmensanwendungen > IDMProv_war > Referenzen auf gemeinsam genutzte Bibliotheken > Zuordnung gemeinsam genutzter Bibliotheken
Ordnet gemeinsam genutzte Bibliotheken einer vollständigen Anwendung oder einem oder mehreren Modulen zu.
Der/dem aufgelisteten Anwendung/Modul Bibliotheken zuordnen
IDMProv
Wählen Sie die Bibliothek in der Liste Verfügbar aus. Durch Anklicken von >> können Sie sie in die Liste Ausgewählt verschieben.
Verfügbar:
IDMUA Classpath
Ausgewählt:
Neu
OK
Abbrechen
Hilfe für Feld
Hilfe für Seite
Fertig
localhost:9043

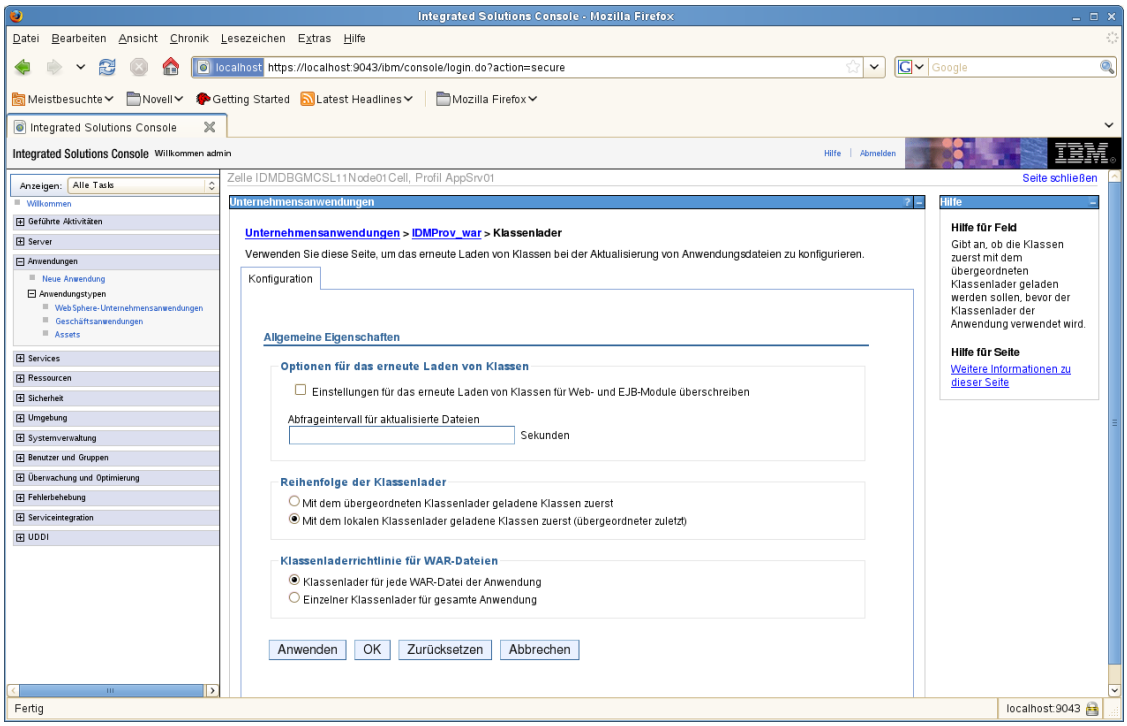
2h Klicken Sie auf *OK*, um zur vorherigen Seite zurückzukehren.

2i Klicken Sie noch einmal auf *OK*.

2j Klicken Sie auf *Speichern*, um die Änderungen an der Serverkonfiguration permanent zu speichern.

2k Starten Sie den Server neu, wenn alle anderen Konfigurationsschritte ausgeführt wurden.

Beachten Sie, dass die Klassenladeänderung auf Anwendungsebene und nicht auf Modulebene vorgenommen werden muss. WebSphere erstellt eine EAR-Datei für die bereitgestellte WAR-Datei und macht die WAR-Datei zu einem Modul innerhalb der EAR-Datei:


Integrated Solutions Console - Mozilla Firefox
Integrated Solutions Console
Unternehmensanwendungen > IDMProv_war > Klassenlader
Verwenden Sie diese Seite, um das erneute Laden von Klassen bei der Aktualisierung von Anwendungsdateien zu konfigurieren.
Konfiguration
Allgemeine Eigenschaften
Optionen für das erneute Laden von Klassen
Einstellungen für das erneute Laden von Klassen für Web- und EJB-Module überschreiben
Abfrageintervall für aktualisierte Dateien
Sekunden
Reihenfolge der Klassenlader
Mit dem übergeordneten Klassenlader geladene Klassen zuerst
Mit dem lokalen Klassenlader geladene Klassen zuerst (übergeordneter zuletzt)
Klassenladerrichtlinie für WAR-Dateien
Klassenlader für jede WAR-Datei der Anwendung
Einzelner Klassenlader für gesamte Anwendung
Anwenden
OK
Zurücksetzen
Abbrechen
Hilfe für Feld
Hilfe für Seite
Fertig
localhost:9043

6.2.3 Importieren der eDirectory-Herkunftsverbürgung in den WebSphere-Keystore

1 Kopieren Sie die eDirectory-Herkunftsverbürgungszertifikate auf den WebSphere-Server.

Bei der Installation der Benutzeranwendung werden die Zertifikate in das Verzeichnis exportiert, in dem Sie die Benutzeranwendung installieren.

2 Importieren Sie die Zertifikate in den WebSphere-Keystore. Sie können dies mithilfe der WebSphere-Administrationskonsole („Zertifikate mit der WebSphere-Administrationskonsole importieren“ auf Seite 110) oder über die Befehlszeile („Zertifikate über die Befehlszeile importieren“ auf Seite 111) tun.

3 Fahren Sie nach dem Importieren der Zertifikate mit Abschnitt 6.3, „Bereitstellung der WAR-Datei“, auf Seite 111 fort.

Zertifikate mit der WebSphere-Administrationskonsole importieren

1 Melden Sie sich bei der Administrationskonsole von WebSphere als Admin-Benutzer an.

2 Rufen Sie in der linken Kontrollleiste *Security* > *SSL Certificate and Key Management* auf.

3. Navigieren Sie in der Liste der Einstellungen auf der rechten Seite zu *Key stores and certificates* unter *Related Items*.
4. Wählen Sie *NodeDefaultTrustStore* (oder den Verbürgungsspeicher, den Sie verwenden).
5. Wählen Sie rechts unter *Additional Properties* die Option *Signer Certificates* aus.
6. Klicken Sie auf *Add*.
7. Geben Sie den Aliasnamen und den vollständigen Pfad zur Zertifikatsdatei ein.
8. Ändern Sie den Datentyp in der Dropdown-Liste in *Binary DER data*.
9. Klicken Sie auf *OK*. Jetzt sollte das Zertifikat in der Liste der Signierzertifikate angezeigt werden.
10. Klicken Sie oben im Bildschirm auf den Link *Save*.

Zertifikate über die Befehlszeile importieren

Führen Sie in der Befehlszeile auf dem Computer, der den WebSphere-Server hostet, das Keytool aus, um das Zertifikat in den WebSphere-Keystore zu importieren.

Hinweis: Sie müssen das WebSphere-Keytool ausführen, damit dies funktioniert. Vergewissern Sie sich außerdem, dass der Store-Typ PKCS12 ist.

Das WebSphere-Keytool befindet sich unter `/IBM/WebSphere/AppServer/java/bin`.

Im Folgenden finden Sie ein Beispiel für einen Keytool-Befehl:

```
keytool -import -trustcacerts -file servercert.der -alias myserveralias -
keystore trust.p12 -storetype PKCS12
```

Wenn sich auf Ihrem System mehrere `trust.p12`-Dateien befinden, müssen Sie ggf. den vollständigen Pfad zu der Datei angeben.

6.2.4 Übergeben der preferIPv4Stack-Eigenschaft an die JVM

Die Benutzeranwendung verwendet JGroups für die Caching-Implementierung. Bei einigen Konfigurationen erfordert JGroups, dass die preferIPv4Stack-Eigenschaft auf „true“ gesetzt wird, um sicherzustellen, dass die mcast_addr-Bindung erfolgreich ist. Ohne diese Option tritt möglicherweise der folgende Fehler auf und das Caching funktioniert nicht ordnungsgemäß:

```
[10/1/09 16:11:22:147 EDT] 0000000d UDP           W org.jgroups.util.Util
createMulticastSocket could not bind to /228.8.8.8 (IPv4 address); make sure
your mcast_addr is of the same type as the IP stack (IPv4 or IPv6).
```

Der Parameter `java.net.preferIPv4Stack=true` ist eine Systemeigenschaft, die auf dieselbe Weise festgelegt werden kann wie andere Systemeigenschaften, wie z. B. `extend.local.config.dir`. Anweisungen zum Festlegen von Systemeigenschaften finden Sie in Abschnitt 6.2.2, „Hinzufügen von Benutzeranwendungs-Konfigurationsdateien und JVM-Systemeigenschaften“, auf Seite 104.

6.3 Bereitstellung der WAR-Datei

Stellen Sie die WAR-Datei mithilfe der WebSphere-Bereitstellungswerkzeuge bereit.

6.3.1 Zusätzliche Konfiguration für WebSphere 7.0

Wenn Sie WebSphere 7.0 mit Version 4.0 des RBPM verwenden, müssen Sie sicherstellen, dass bestimmte JAR-Dateien (wie beispielsweise commons-digester.jar) in dieser Version von RBPM jeweils auf die neueste verfügbare Version aktualisiert wurden. Aus diesem Grund können Versionskonflikte mit JAR-Dateien auftreten, die mit WebSphere mitgeliefert wurden, wenn Sie Ihre Umgebung nicht ordnungsgemäß konfigurieren.

Sie müssen Ihren WebSphere-Server so konfigurieren, dass er die Klassen zuerst aus der Datei „IDMProv.war“ lädt, um sicherzustellen, dass Sie die richtigen JAR-Dateien verwenden. Für die Datei „IDMProv.war“ müssen Sie die Option *Classes loaded with local class loader first (parent last)* auswählen.

6.4 Starten der und Zugriff auf die Benutzeranwendung

So starten Sie die Benutzeranwendung:

1. Melden Sie sich bei der Administrationskonsole von WebSphere als Admin-Benutzer an.
2. Wählen Sie in der linken Navigationsleiste *Applications* > *Enterprise Applications*.
3. Wählen Sie das Kontrollkästchen neben der Anwendung aus, die Sie starten möchten, und klicken Sie anschließend auf *Start*.

   Nach dem Start wird in der Spalte *Application status* ein grüner Pfeil angezeigt.

So greifen Sie auf die Benutzeranwendung zu:

1. Sie können mithilfe des Kontexts, den Sie während der Bereitstellung festgelegt haben, auf das Portal zugreifen.

   Der Standardport für den Web-Container auf WebSphere ist 9080 bzw. 9443 für den sicheren Port. Die URL hat das folgende Format: `http:// <Server>:9080/IDMProv`

Installieren der Benutzeranwendung auf WebLogic

7

Das WebLogic-Installationsprogramm konfiguriert die Benutzeranwendungs-WAR-Datei basierend auf Ihrer Eingabe. In diesem Abschnitt finden Sie Details zu folgenden Themen:

- Abschnitt 7.1, „WebLogic-Installations-Checkliste“, auf Seite 113
- Abschnitt 7.2, „Installieren und Konfigurieren der Benutzeranwendungs-WAR“, auf Seite 114
- Abschnitt 7.3, „Vorbereiten der WebLogic-Umgebung“, auf Seite 128
- Abschnitt 7.4, „Bereitstellen der Benutzeranwendungs-WAR-Datei“, auf Seite 131
- Abschnitt 7.5, „Zugriff auf die Benutzeranwendung“, auf Seite 132

Informationen zum Installieren mithilfe einer nicht-grafischen Benutzeroberfläche finden Sie unter Kapitel 8, „Installation von der Konsole aus oder mit einem einzigen Befehl“, auf Seite 133.

Führen Sie das Installationsprogramm als Nicht-root-Benutzer aus.

Datenmigration. Weitere Informationen zur Migration finden Sie im *Benutzeranwendung: Migrationshandbuch* (http://www.novell.com/documentation/idm40/index.html).

7.1 WebLogic-Installations-Checkliste

- ❑ Installieren Sie WebLogic.

  Befolgen Sie die Installationsanweisungen in der WebLogic-Dokumentation.

- ❑ Erstellen Sie eine WebLogic-fähige WAR-Datei.

  Führen Sie diese Aufgabe mithilfe des Installationsprogramms der Identity Manager-Benutzeranwendung durch. Weitere Informationen hierzu finden Sie unter Abschnitt 7.2, „Installieren und Konfigurieren der Benutzeranwendungs-WAR“, auf Seite 114.

- ❑ Bereiten Sie die WebLogic-Umgebung für die WAR-Bereitstellung vor, indem Sie die Konfigurationsdateien an die entsprechenden WebLogic-Speicherorte kopieren.

  Weitere Informationen hierzu finden Sie unter Abschnitt 7.3, „Vorbereiten der WebLogic-Umgebung“, auf Seite 128.

- ❑ Stellen Sie die WAR-Datei bereit.

  Weitere Informationen hierzu finden Sie unter Abschnitt 7.4, „Bereitstellen der Benutzeranwendungs-WAR-Datei“, auf Seite 131.

7.2 Installieren und Konfigurieren der Benutzeranwendungs-WAR

Hinweis: Für WebLogic 10.3 benötigt das Installationsprogramm das Java 2 Platform Standard Edition Development Kit Version 1.6 JDK von JRockit. Falls Sie eine andere Version verwenden, wird die Benutzeranwendungs-WAR-Datei nicht erfolgreich konfiguriert. Die Installation scheint erfolgreich zu verlaufen, Sie erhalten aber Fehlermeldungen, wenn Sie die Benutzeranwendung starten.

1. Rufen Sie das Verzeichnis mit den Installationsdateien auf.
2. Starten Sie das Installationsprogramm für Ihre Plattform von der Befehlszeile aus unter Verwendung der JRockit Java-Umgebung (mit Version 1.6_17):

   Solaris

   ```
   $ /opt/WL/bea/jrockit_160_17/bin/java -jar IdmUserApp.jar
   ```

   Windows

   ```
   C:\WL\bea\jrockit_160_17\bin\java -jar IdmUserApp.jar
   ```

   Wenn das Installationsprogramm startet, werden Sie nach der Sprache gefragt.

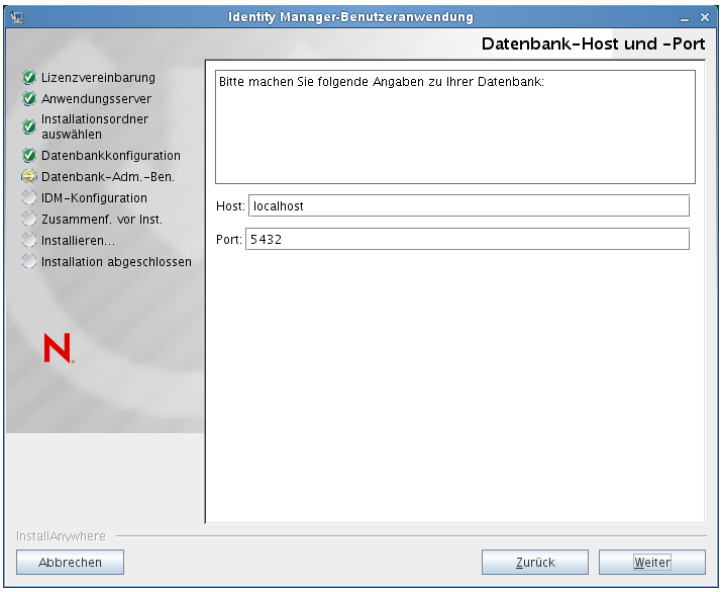
3. Verwenden Sie die nachfolgenden Informationen, um die Sprache auszuwählen, die Lizenzvereinbarung zu akzeptieren und die Anwendungsserverplattform auszuwählen:

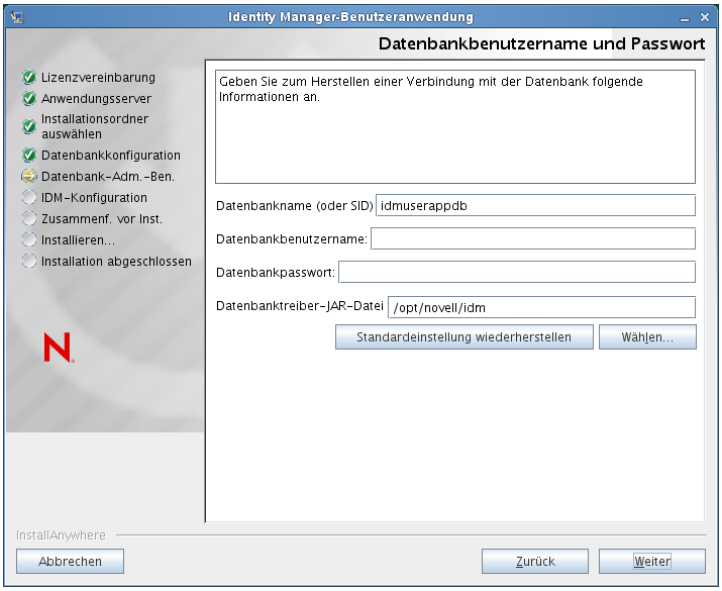
Installationsbildschirm	Beschreibung
Benutzeranwendungsinstallation	Wählen Sie die Sprache für das Installationsprogramm. Die Standardeinstellung ist „Englisch“.
Lizenzvereinbarung	Lesen Sie die Lizenzvereinbarung und klicken Sie auf *Lizenzvertrag zustimmen*.

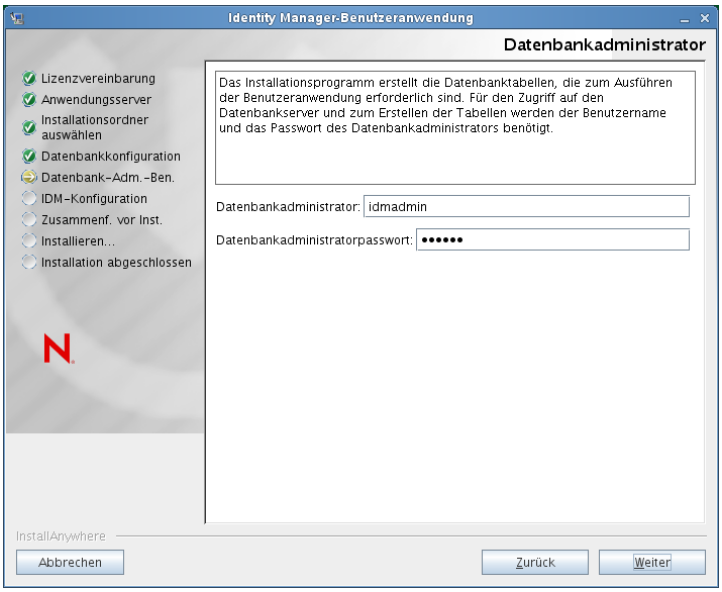
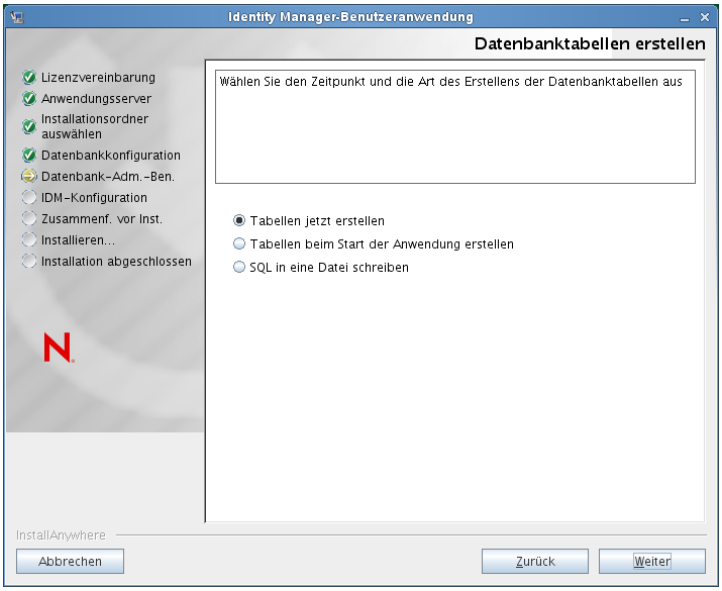
Installationsbildschirm	Beschreibung
Anwendungsserverplattform	Wählen Sie *WebLogic.* Wenn sich die WAR-Datei der Benutzeranwendung nicht im selben Verzeichnis befindet wie das Installationsprogramm, werden Sie aufgefordert, den Pfad zur WAR-Datei einzugeben. Wenn sich die WAR-Datei am Standardspeicherort befindet, können Sie auf *Standarddatei wiederherstellen* klicken. Sie können stattdessen auch auf die Schaltfläche zum *Auswählen* klicken und einen Speicherort auswählen, um den Speicherort der WAR-Datei anzugeben. Wenn Sie die Installation auf WebLogic durchführen, müssen Sie das Installationsprogramm mithilfe der Java-Umgebung von BEA (jrockit) starten. Wenn Sie WebLogic als Anwendungsserver wählen und nicht jrockit zum Starten der Installation verwenden, erscheint eine Fehlermeldung und die Installation wird beendet:

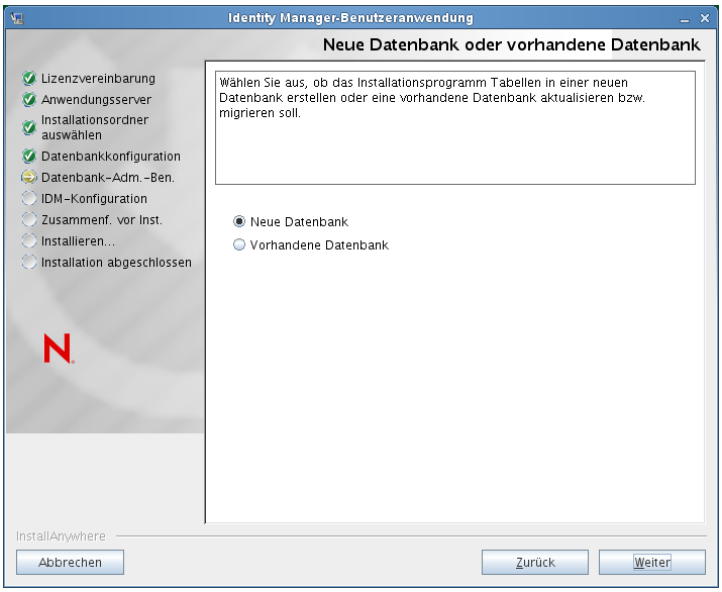
4 Verwenden Sie die nachfolgenden Informationen, um die Installationsart zu wählen, einen Installationsordner auszuwählen und die Datenbank zu konfigurieren:

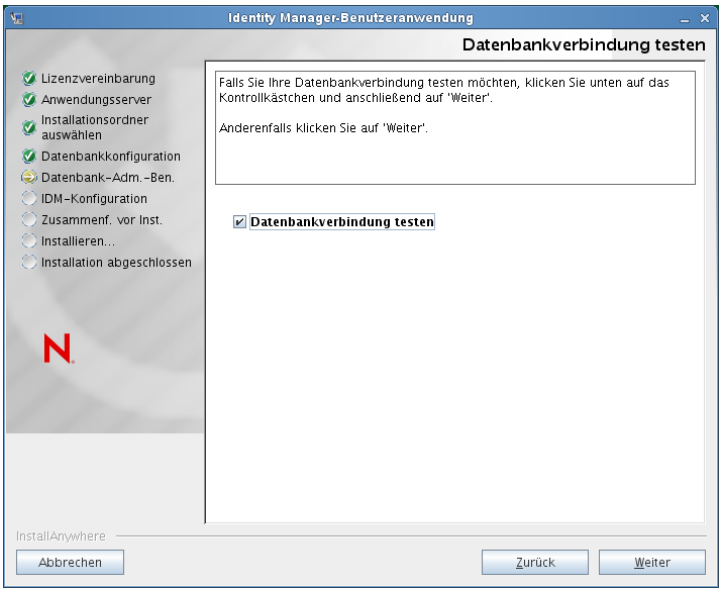
Installationsbildschirm	Beschreibung
Installationstyp	*Rollenbasierte Bereitstellung*: Wählen Sie diese Option aus, um das rollenbasierte Bereitstellungsmodul zu installieren. In dieser Version wird nur diese Installationsart unterstützt.
Installationsordner auswählen	Geben Sie an, wo das Installationsprogramm die Dateien speichern soll.
Datenbankplattform	Wählen Sie die Datenbankplattform. Die Datenbank- und JDBC-Treiber müssen bereits installiert sein. Für WebLogic gibt es folgende Optionen: ◆ Oracle ◆ Microsoft SQL Server ◆ PostgreSQL

Installationsbildschirm	Beschreibung
Datenbank-Host und Port	*Host*: Geben Sie den Hostnamen oder die IP-Adresse des Datenbankservers an. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied derselbe Hostname bzw. dieselbe IP-Adresse angegeben werden. *Port*: Geben Sie die Listener-Portnummer der Datenbank an. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied derselbe Port angegeben werden. 

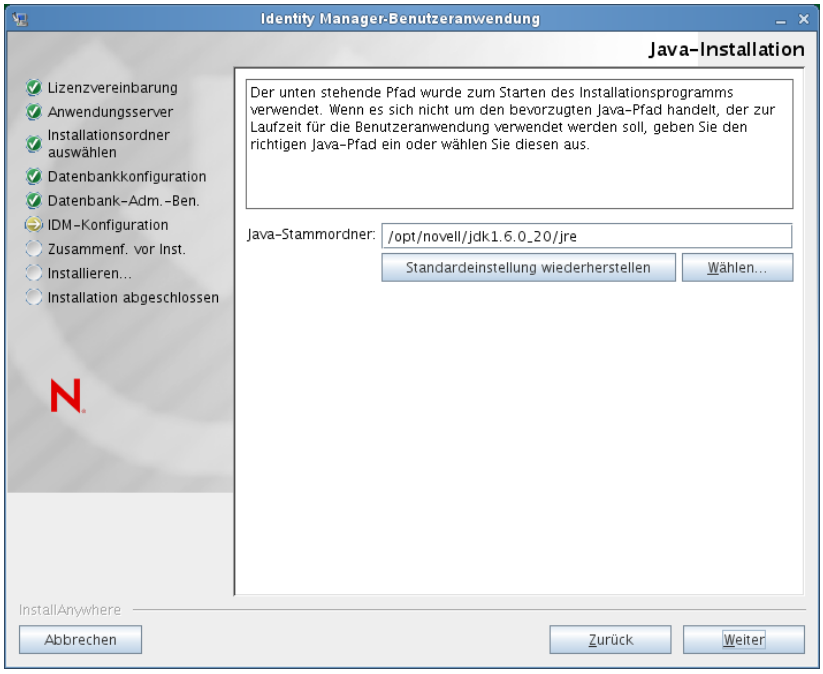
Installationsbildschirm	Beschreibung
Datenbankbenutzername und Passwort	*Datenbankname* (oder SID): Geben Sie für MS SQL Server oder PostgreSQL den Namen Ihrer vorkonfigurierten Datenbank an. Geben Sie für Oracle den zuvor erstellten Oracle System Identifier (SID) ein. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied derselbe Datenbankname bzw. derselbe SID angegeben werden. *Datenbankbenutzer*name: Geben Sie den Datenbankbenutzer an. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied dieselbe Datenbank angegeben werden. *Datenbankpasswort*: Geben Sie das Datenbankpasswort an. In einer Clusterkonfiguration muss für jedes Cluster-Mitglied dasselbe Passwort angegeben werden. *Datenbanktreiber-JAR-Datei* Geben Sie die Thin-Client-JAR-Datei für den Datenbankserver an. Dieser ist erforderlich. 

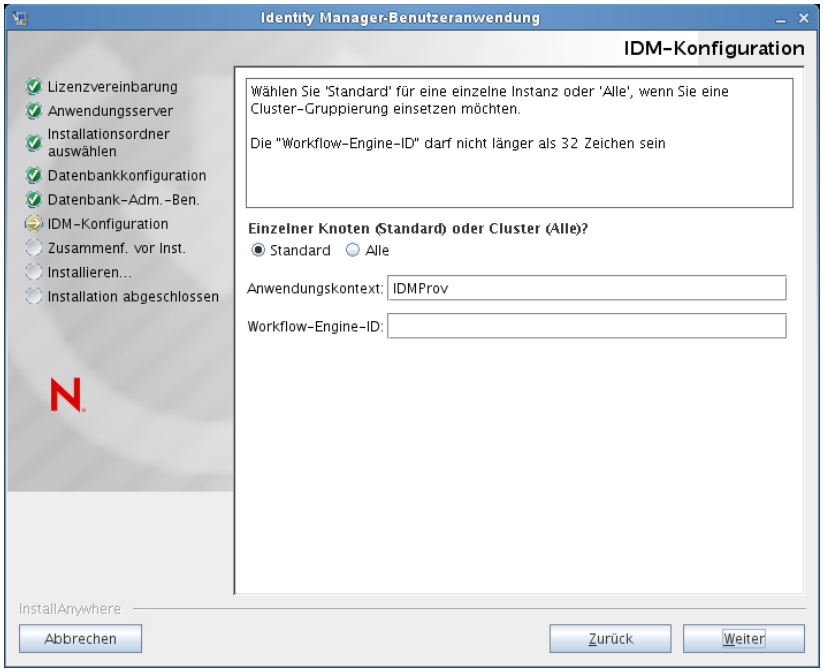
Installationsbildschirm	Beschreibung
Datenbankadministrator	Dieser Bildschirm ist bereits mit dem auf der Seite „Datenbankbenutzername und Passwort“ angegebenen Benutzernamen und Passwort ausgefüllt. Falls der angegebene Datenbankbenutzer nicht über die erforderlichen Berechtigungen zum Erstellen von Tabellen auf dem Datenbankserver verfügt, muss eine andere Benutzer-ID mit den erforderlichen Rechten eingegeben werden. 
Datenbanktabellen erstellen	Geben Sie an, wann die Datenbanktabellen erstellt werden sollen: 

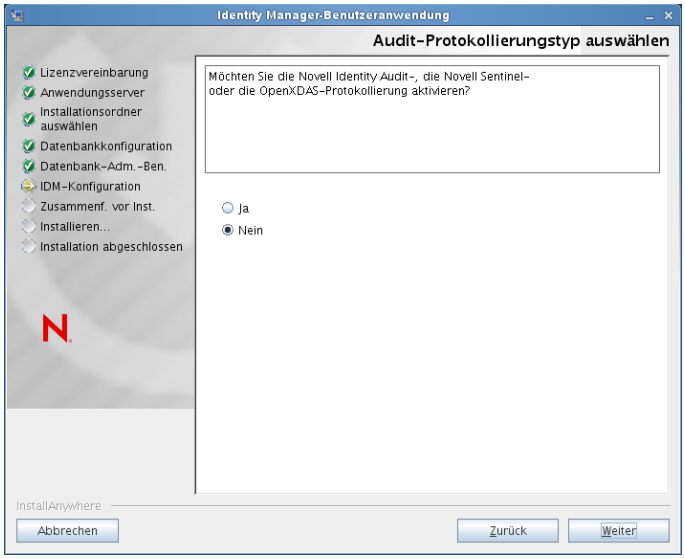
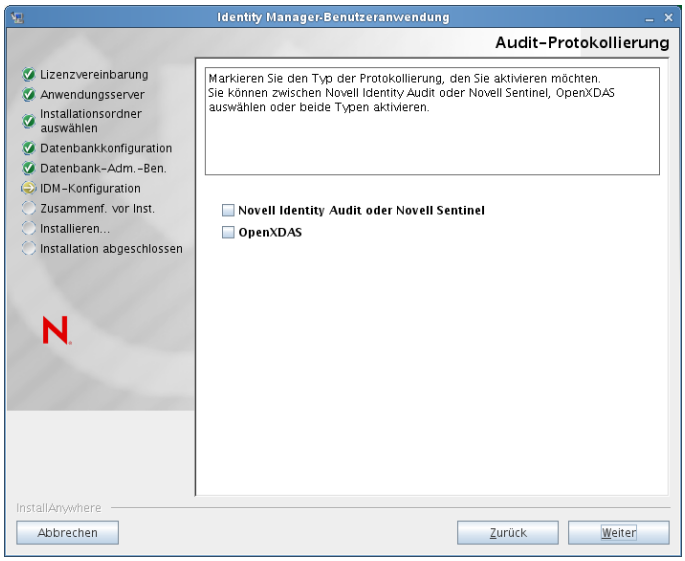
Installationsbildschirm	Beschreibung
Neue Datenbank oder vorhandene Datenbank	Falls die zu verwendende Datenbank neu oder leer ist, klicken Sie auf *Neue Datenbank*. Wenn es sich bei der Datenbank um eine Datenbank einer vorherigen Installation handelt, klicken Sie auf *Vorhandene Datenbank*. 

Installationsbildschirm	Beschreibung
Datenbankverbindung testen	Sie können zum Sicherstellen, dass die Informationen in den vorherigen Bildschirmen korrekt sind, die Datenbankverbindung testen, indem Sie das Kontrollkästchen *Datenbankverbindung testen* aktivieren:  Das Installationsprogramm muss sowohl zum direkten Erstellen von Tabellen als auch zum Erstellen der .SQL-Datei eine Verbindung zur Datenbank herstellen. Wenn Sie die Datenbankverbindung testen und der Test fehlschlägt, können Sie dennoch mit der Installation fortfahren. In diesem Fall müssen Sie die Tabellen nach der Installation erstellen, wie im *Benutzeranwendung: Administrationshandbuch* (http://www.novell.com/documentation/idm40/agpro/?page=/documentation/idm40/agpro/data/bncf7rj.html) beschrieben.

5 Verwenden Sie die nachfolgenden Informationen, um Java und IDM sowie die Audit-Einstellungen und die Sicherheit zu konfigurieren.

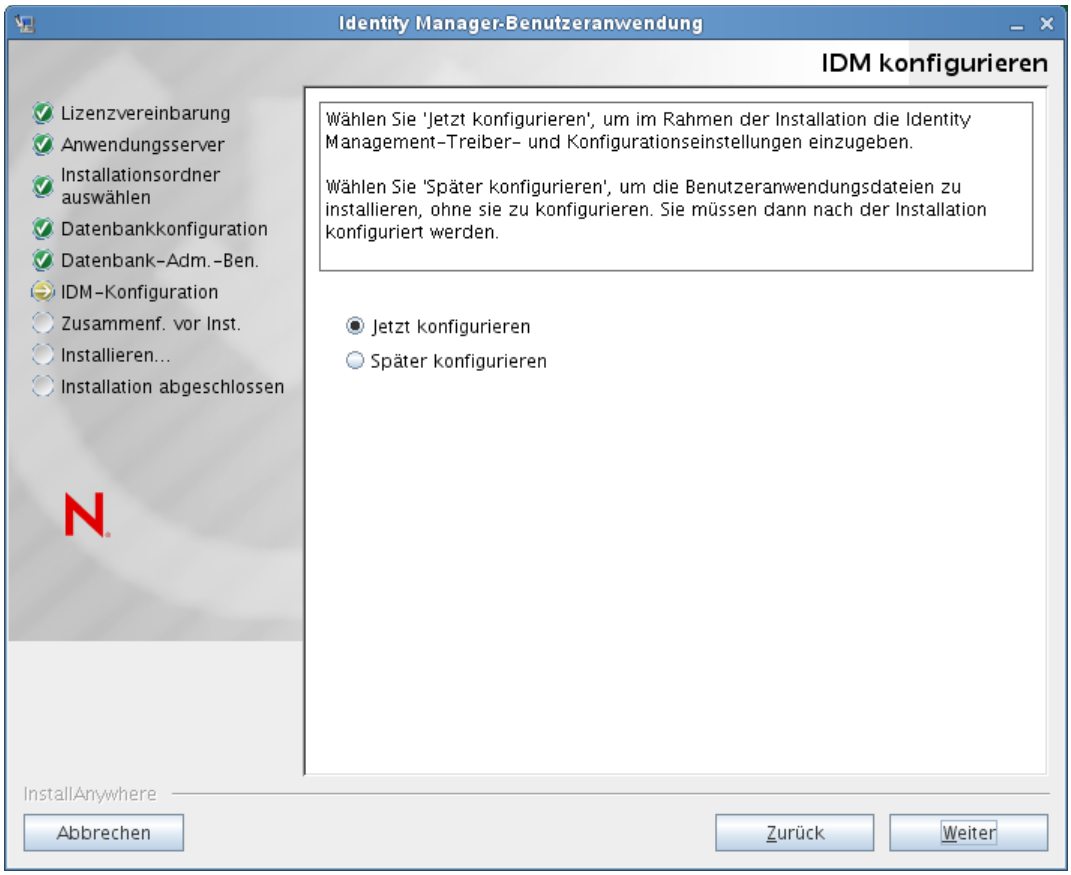
Installationsbildschirm	Beschreibung
Java-Installation	Geben Sie den Java-Stamminstallationsordner an. Die Java-Installation gibt anhand des Werts der Umgebungsvariablen „JAVA_HOME“ den Java-Pfad an und bietet Ihnen die Möglichkeit, den Pfad ggf. zu korrigieren:  Zu diesem Zeitpunkt überprüft das Installationsprogramm, ob die ausgewählte Java-Umgebung für den ausgewählten Anwendungsserver korrekt ist. Zudem wird überprüft, ob das Installationsprogramm in die cacerts-Datei der angegebenen JRE schreiben kann.

Installationsbildschirm	Beschreibung
IDM-Konfiguration	Wählen Sie den Anwendungsserver-Konfigurationstyp: ◆ Wählen Sie *Standard*, wenn diese Installation für einen einzelnen Knoten erfolgt, der nicht Teil eines Clusters ist. Wenn Sie *Standard* auswählen und zu einem späteren Zeitpunkt einen Cluster benötigen, müssen Sie die Benutzeranwendung erneut installieren. ◆ Wählen Sie *Alle*, wenn diese Installation für ein Cluster erfolgt. *Anwendungskontext*: Der Name der Anwendungsserver-Konfiguration, der Name der WAR-Datei der Anwendung und der Name des URL-Kontexts. Das Installations-Skript erstellt eine Serverkonfiguration und benennt die Konfiguration standardmäßig auf der Basis des *Anwendungsnamens*. Notieren Sie den Anwendungsnamen und fügen Sie ihn in die URL ein, wenn Sie die Benutzeranwendung über einen Browser starten. 

Installationsbildschirm	Beschreibung
Audit-Protokollierungstyp auswählen	Klicken Sie auf *Ja*, um die Protokollierung zu aktivieren. Klicken Sie auf *Nein*, um die Protokollierung zu deaktivieren.  Im nächsten Teilfenster werden Sie aufgefordert, den Typ für die Protokollierung anzugeben. Treffen Sie eine Auswahl aus den folgenden Optionen: ◆ *Novell Identity Audit oder Novell Sentinel*: Ermöglicht die Protokollierung über einen Novell Auditing-Client für die Benutzeranwendung. ◆ *OpenXDAS*: Ereignisse werden auf Ihrem OpenXDAS-Protokollierungsserver protokolliert. Weitere Informationen zum Einrichten der Protokollierung finden Sie im *Benutzeranwendung: Administrationshandbuch*. 

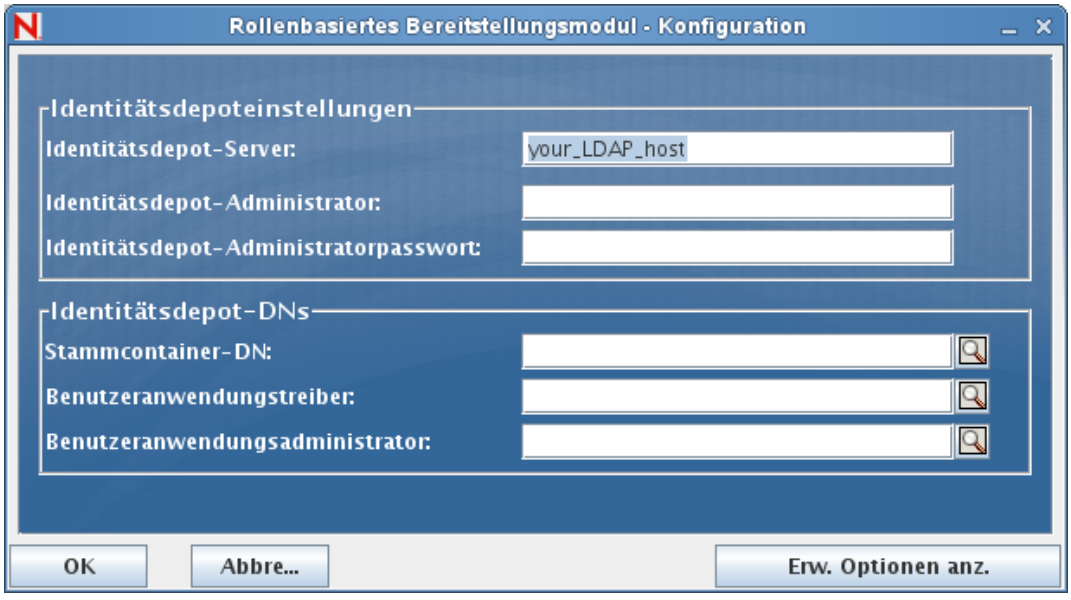
Installationsbildschirm	Beschreibung
Novell Identity Audit oder Novell Sentinel	*Server*: Geben Sie den Hostnamen oder die IP-Adresse des Servers an, sofern Sie die Protokollierung aktivieren. Wenn Sie die Protokollierung deaktivieren, wird dieser Wert ignoriert. *Ordner für Cache-Protokoll*: Geben Sie das Verzeichnis für den Protokollierungs-Cache-Speicher an.
Sicherheit - Master-Schlüssel	*Ja*: Erlaubt den Import eines vorhandenen Master-Schlüssels. Wenn ein vorhandener verschlüsselter Master-Schlüssel importiert werden soll, kopieren Sie den Schlüssel und fügen Sie ihn in das Fenster des Installationsvorgangs ein. *Nein*: Erstellt einen neuen Master-Schlüssel. Nach Abschluss der Installation müssen Sie den Master-Schlüssel manuell speichern, wie in Abschnitt 9.1, „Aufzeichnen des Master-Schlüssels“, auf Seite 149 beschrieben. Bei der Installation wird der verschlüsselte Master-Schlüssel im Installationsverzeichnis in die Datei `master-key.txt` geschrieben. Mögliche Gründe für den Import eines vorhandenen Master-Schlüssels: ◆ Sie verlagern Ihre Installation aus einem Staging-System in ein Produktionssystem und möchten auch weiterhin auf die Datenbank des Staging-Systems zugreifen. ◆ Sie haben die Benutzeranwendung als erstes Mitglied eines Clusters installiert und führen nun die Installation auf nachfolgenden Cluster-Mitgliedern durch (für die derselbe Master-Schlüssel benötigt wird). ◆ Bedingt durch einen Festplattenfehler müssen Sie die Benutzeranwendung wiederherstellen. Sie müssen die Benutzeranwendung neu installieren und den Master-Schlüssel der vorherigen Installation angeben. Auf diese Weise erhalten Sie Zugriff auf zuvor gespeicherte verschlüsselte Daten.

6 Wenn Sie RBPM jetzt konfigurieren möchten, wählen Sie *Jetzt konfigurieren* aus und klicken Sie auf *Weiter*.



(Wenn Sie nicht zur Eingabe dieser Informationen aufgefordert werden, haben Sie möglicherweise die in Abschnitt 2.5, „Installieren des Java Development Kit“, auf Seite 32 aufgeführten Schritte nicht ausgeführt.)

Die Standardansicht des Konfigurationsfensters für das rollenbasierte Bereitstellungsmodul enthält diese sechs Felder:



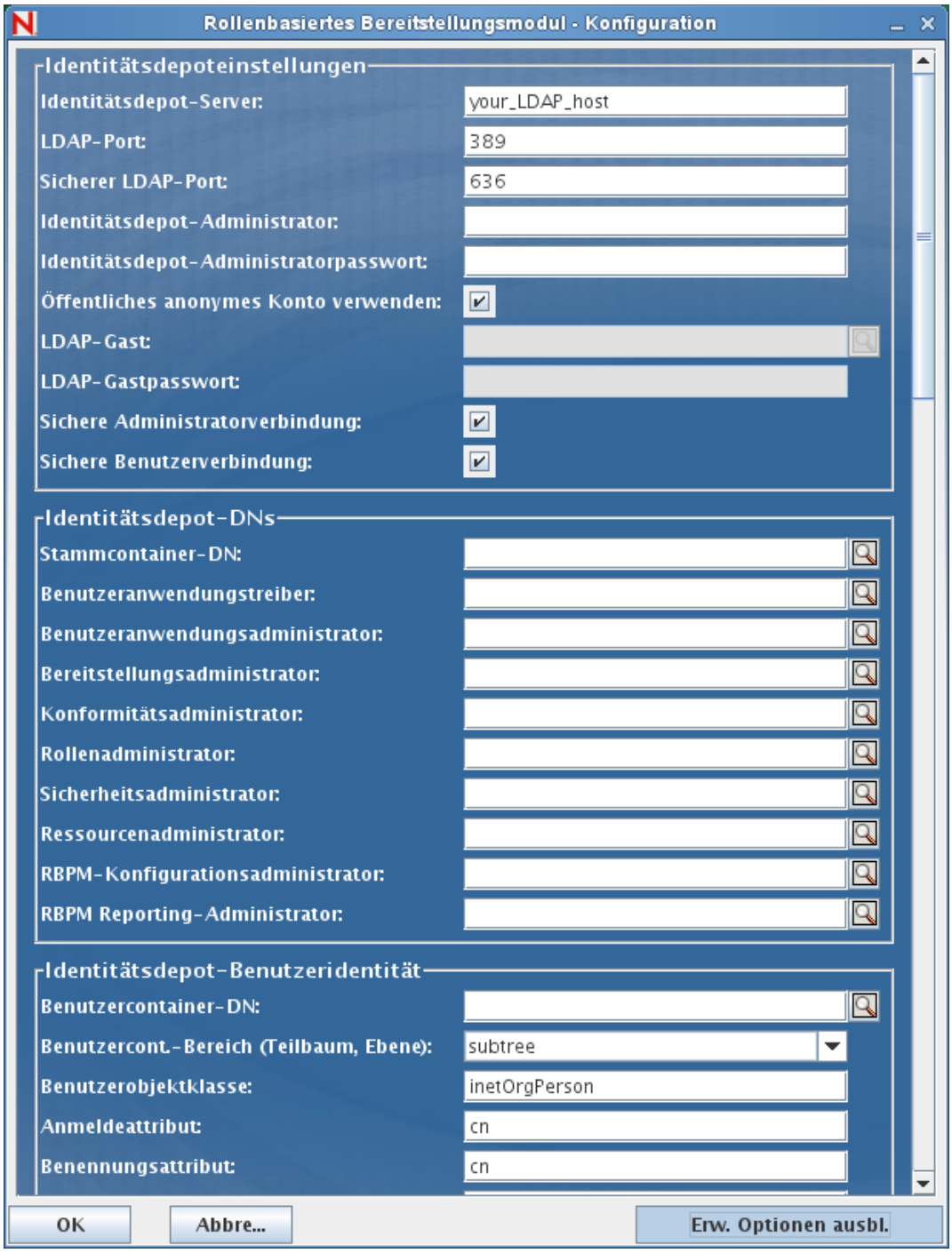
Das Installationsprogramm übernimmt den Wert aus der Stammcontainer-DN und wendet ihn auf die folgenden Werte an:

- Benutzercontainer-DN
- Gruppencontainer-DN

Das Installationsprogramm übernimmt den Wert aus den Benutzeranwendungsadministratorfeldern und wendet ihn auf die folgenden Werte an:

- Bereitstellungsadministrator
- Konformitätsadministrator
- Rollenadministrator
- Sicherheitsadministrator
- Ressourcenadministrator
- RBPM-Konfigurationsadministrator

Wenn Sie diese Werte explizit angeben möchten, klicken Sie auf *Erweiterte Optionen anzeigen* und ändern Sie sie:



Bei der Installation der Benutzeranwendung können Sie Konfigurationsparameter für die Benutzeranwendung festlegen. Die meisten dieser Parameter können auch nach der Installation in der Datei `configupdate.sh` oder `configupdate.bat` bearbeitet werden. Auf Ausnahmen wird in den Parameterbeschreibungen hingewiesen.

Unter Anhang A, „IDM Benutzeranwendung - Konfigurationsreferenz“, auf Seite 157 finden Sie eine Beschreibung für jede Option.

7 Mithilfe der folgenden Informationen wird die Installation ausgeführt.

Installationsbildschirm	Beschreibung
Zusammenfassung vor der Installation	Überprüfen Sie auf der Seite „Zusammenfassung vor der Installation“ die Einstellungen der Installationsparameter. Wenn Sie Änderungen vornehmen möchten, können Sie über die Schaltfläche *Zurück* vorherige Installationsseiten aufrufen. Die Werte auf der Seite „Benutzeranwendung - Konfiguration“ werden nicht gespeichert, daher müssen Sie die Einstellungen auf dieser Seite erneut vornehmen, wenn Sie vorherige Seiten des Installationsvorgangs ändern. Wenn Sie die gewünschten Änderungen an den Installations- und Konfigurationsparametern vorgenommen haben, kehren Sie zur Seite „Zusammenfassung vor der Installation“ zurück und klicken Sie auf *Installieren*.
Installation abgeschlossen	Zeigt an, dass die Installation abgeschlossen ist.

7.2.1 Anzeigen der Installations- und Protokolldateien

Wenn die Installation ohne Fehler abgeschlossen wurde, fahren Sie mit Vorbereiten der WebLogic-Umgebung fort. Sofern bei der Installation Fehler- oder Warnmeldungen ausgegeben wurden, ermitteln Sie die Probleme anhand der Protokolldateien:

- Die Datei `Identity_Manager_User_Application_InstallLog.log` enthält die Ergebnisse der wichtigsten Installationsaufgaben.
- Die Datei `Novell-Custom-Install.log` enthält Informationen zur Konfiguration der Benutzeranwendung, die während der Installation vorgenommen wurde.

7.3 Vorbereiten der WebLogic-Umgebung

- Abschnitt 7.3.1, „Konfiguration des Verbindungspools“, auf Seite 128
- Abschnitt 7.3.2, „Angeben von Speicherorten für die RBPM-Konfigurationsdateien“, auf Seite 129
- Abschnitt 7.3.3, „Entfernen von OpenSAML JAR-Dateien“, auf Seite 131
- Abschnitt 7.3.4, „Workflow-Plugin und WebLogic-Setup“, auf Seite 131

7.3.1 Konfiguration des Verbindungspools

- ❑ Kopieren Sie die JAR-Dateien des Datenbanktreibers in die Domäne, auf der Sie die Benutzeranwendung bereitstellen möchten.
- ❑ Erstellen Ihrer Datenquelle.

  Befolgen Sie die Anweisungen zum Erstellen einer Datenquelle in der WebLogic-Dokumentation.

  Beachten Sie, dass der JNDI-Name für die Datenquelle `jdbc/IDMUADataSource` lauten muss, ungeachtet des Namens, den Sie beim Erstellen der Benutzeranwendungs-WAR-Datei für die Datenquelle oder die Datenbank angegeben haben.

7.3.2 Angeben von Speicherorten für die RBPM-Konfigurationsdateien

Die WebLogic-Benutzeranwendung benötigt Informationen zum Auffinden der Dateien `sys-configuration-xmldata.xml`, `idmuserapp_logging.xml` und `wl_idmuserapp_logging.xml`. Deshalb müssen Sie den Speicherort der Dateien zur Datei `setDomainEnv.cmd` hinzufügen.

Wenn Sie die Speicherorte in der Datei `setDomainEnv.cmd` oder `setDomainEnv.sh` angeben, werden diese Informationen dem Anwendungsserver zur Verfügung gestellt:

1. Öffnen Sie `setDomainEnv.cmd` oder `setDomainEnv.sh`.
2. Suchen Sie die Zeile, die wie folgt aussieht:

   ```
   set JAVA_PROPERTIES
   export JAVA_PROPERTIES
   ```

3. Fügen Sie unter dem Eintrag JAVA_PROPERTIES Einträge für Folgendes hinzu:

   - `-Dextend.local.config.dir==<Verzeichnispfad>`: Geben Sie den Ordner (nicht die Datei selbst) an, in dem sich die Datei `sys-configuration.xml` befindet.
   - `-Didmuserapp.logging.config.dir==<Verzeichnispfad>`: Geben Sie den Ordner (nicht die Datei selbst) an, in dem sich die Datei `idmuserapp_logging.xml` befindet.
   - `-Dlog.init.file==<Dateiname>`: Geben Sie die Datei `wl_idmuserapp_logging.xml` an, die für die log4j-Konfiguration verwendet wird. Diese Datei handhabt die erforderlichen Appender- und Logger-Konfigurationen für die Benutzeranwendung in Situationen, in denen mehrere Anwendungen auf demselben Anwendungsserver installiert sind.

   Zum Beispiel unter Windows:

   ```
   set JAVA_OPTIONS=-Dextend.local.config.dir=c:\novell\idm
   set JAVA_OPTIONS=%JAVA_OPTIONS% -
   Didmuserapp.logging.config.dir=c:\novell\idm
   set JAVA_OPTIONS=%JAVA_OPTIONS%
   -Dlog.init.file=wl_idmuserapp_logging.xml
   ```

4. Legen Sie die Umgebungsvariable `EXT_PRE_CLASSPATH` so fest, dass sie auf die folgenden JAR-Dateien verweist:

   - `antlr-2.7.6.jar`
   - `log4j.jar`
   - `commons-logging.jar`

     Hinweis: Sie müssen diese JAR-Datei von der Apache-Website herunterladen.

   - `xalan.jar`
   - `xercesImpl.jar`
   - `xsltc.jar`
   - `serializer.jar`
   - `IDMselector.jar`

Hinweis: Ein alternativer Ansatz zum Hinzufügen dieser JAR-Dateien zur Variablen EXT_PRE_CLASSPATH besteht darin, diese Dateien in das Verzeichnis „WEB-INF/lib“ innerhalb der Datei „IDMProv.war“ zu kopieren.

4a Suchen Sie diese Zeile:

```
ADD EXTENSIONS TO CLASSPATH
```

4b Fügen Sie `EXT_PRE_CLASSPATH` unterhalb der Zeile hinzu. Zum Beispiel unter Windows:

```
set
EXT_PRE_CLASSPATH=C:\bea\user_projects\domains\base_domain\lib\antlr-
2.7.6.jar;C:\bea\user_projects\domain\base_domain\lib\log4j.jar;C:\be
a\user_projects\domains\base_domain\lib\commons-
logging.jar;C:\bea\user_projects\domains\base_domain\lib\xalan.jar;C:
\bea\user_projects\domains\base_domain\lib\xercesImpl.jar;C:\bea\user
_projects\domains\base_domain\lib\xsltc.jar;C:\bea\user_projects\doma
ins\base_domain\lib\serializer.jar
```

Zum Beispiel unter Linux:

```
export EXT_PRE_CLASSPATH=/opt/bea/user_projects/domains/base_domain/
lib/antlr-2.7.6.jar:/opt/bea/user_projects/domain/base_domain/lib/
log4j.jar:/opt/bea/user_projects/domains/base_domain/lib/commons-
logging.jar:/opt/bea/user_projects/domains/base_domain/lib/
xalan.jar:/opt/bea/user_projects/domains/base_domain/lib/
xercesImpl.jar:/opt/bea/user_projects/domains/base_domain/lib/
xsltc.jar:/opt/bea/user_projects/domains/base_domain/lib/
serializer.jar
```

5 Speichern und schließen Sie die Datei.

Die XML-Dateien werden auch vom Dienstprogramm „ConfigUpdate“ verwendet. Daher müssen Sie die Datei `configupdate.bat` oder `configupdate.sh` folgendermaßen bearbeiten:

1 Öffnen Sie `configupdate.bat` oder `configupdate.sh`.

2 Suchen Sie die folgende Zeile:

```
-Duser.language=en -Duser.region="
```

3 Ändern Sie die vorhandene Zeile dahingehend, dass sie den Pfad zur Datei „sys-configuration.xml“ enthält:

Zum Beispiel unter Windows:

```
-Dextend.local.config.dir=c:\novell\idm
```

Zum Beispiel unter Linux:

```
-Dextend.local.config.dir=/opt/novell/idm
```

4 Speichern und schließen Sie die Datei.

5 Führen Sie das Dienstprogramm „ConfigUpdate“ aus, um das Zertifikat in den Keystore des JDK unter BEA_HOME zu installieren.

Wenn Sie `configupdate` ausführen, werden Sie nach der Datei `cacerts` unter dem von Ihnen verwendeten JDK gefragt. Wenn Sie nicht das gleiche JDK verwenden, das während der Installation angegeben wurde, müssen Sie `configupdate` für die WAR-Datei ausführen. Achten Sie auf das angegebene JDK, da dieser Eintrag auf das von WebLogic verwendete JDK zeigen muss. Hiermit wird eine Zertifikatsdatei für die Verbindung zum Identitätsdepot importiert. Der Zweck besteht darin, eine Zertifikatsdatei für die Verbindung mit eDirectory zu importieren.

Der Wert für die Identitätsdepot-Zertifikate im Dienstprogramm „configupdate“ muss auf den folgenden Speicherort verweisen:

```
c:\jrockit\jre\lib\security\cacerts
```

7.3.3 Entfernen von OpenSAML JAR-Dateien

Die OpenSAML JAR-Dateien, die WebLogic verwendet, stehen im Widerspruch zu denjenigen, die für die Benutzeranwendung benötigt werden. Deshalb müssen Sie die OpenSAML JAR-Dateien im Verzeichnis „WebLogic/WL103/modules“ entfernen, um sicherzustellen, dass die Benutzeranwendung ordnungsgemäß auf WebLogic bereitgestellt wird. Diese Anforderung gilt für alle Benutzeranwendungen, bei denen SSO nicht aktiviert ist.

Stellen Sie sicher, dass Sie die folgenden JAR-Dateien im Verzeichnis „WebLogic/WL103/modules“ entfernen:

```
com.bea.core.bea.opensaml_1.0.0.0_5-0-2-0.jar
com.bea.core.bea.opensaml2_1.0.0.0_5-0-2-0.jar
```

7.3.4 Workflow-Plugin und WebLogic-Setup

Das Workflow-Administration-Plugin für iManager kann keine Verbindung zum Benutzeranwendungstreiber herstellen, der auf WebLogic ausgeführt wird, wenn das `enforce-valid-basic-auth-credentials`-Flag auf „true“ gesetzt ist. Damit diese Verbindung erfolgreich ist, müssen Sie dieses Flag deaktivieren.

Führen Sie zur Deaktivierung des enforce-valid-basic-auth-credentials-Flags folgende Schritte durch:

1. Öffnen Sie die Datei `config.xml` im Ordner `<WLHome>\user_projects\domains\idm\config\`.
2. Fügen Sie die folgende Zeile zum Abschnitt `<security-configuration>` hinzu, und zwar direkt vor dem Ende dieses Abschnitts:

   ```
   <enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>
   </security-configuration>
   ```
3. Speichern Sie die Datei und starten Sie den Server neu.

Nachdem Sie diese Änderung durchgeführt haben, sollten Sie sich im Workflow-Administration-Plugin anmelden können.

7.4 Bereitstellen der Benutzeranwendungs-WAR-Datei

Zu diesem Zeitpunkt können Sie die Benutzeranwendungs-WAR-Datei mithilfe des standardmäßigen WebLogic-Bereitstellungsverfahrens bereitstellen.

7.5 Zugriff auf die Benutzeranwendung

- Navigieren Sie zur Benutzeranwendungs-URL:

  ```
  http://application-server-host:port/application-context
  ```

  Beispiel:

  ```
  http://localhost:8180/IDMProv
  ```

Installation von der Konsole aus oder mit einem einzigen Befehl

8

In diesem Abschnitt werden die Installationsmethoden beschrieben, die Sie statt der Installation über eine grafische Benutzeroberfläche (siehe Kapitel 5, „Installieren der Benutzeranwendung auf JBoss“, auf Seite 59) verwenden können. Es werden u. a. folgende Themen erläutert:

- Abschnitt 8.1, „Installation der Benutzeranwendung von der Konsole aus“, auf Seite 133
- Abschnitt 8.2, „Installation der Benutzeranwendung mit einem einzigen Befehl“, auf Seite 134
- Abschnitt 8.3, „Ausführen des JBossPostgreSQL-Dienstprogramms im Automatik- oder im Konsolenmodus“, auf Seite 145
- Abschnitt 8.4, „Ausführen des RIS-Installationsprogramms im Automatik- oder im Konsolenmodus“, auf Seite 146

8.1 Installation der Benutzeranwendung von der Konsole aus

In diesem Abschnitt wird die Installation der Identity Manager-Benutzeranwendung über die Konsolenversion (Befehlszeile) des Installationsprogramms erläutert.

Hinweis: Das Installationsprogramm erfordert mindestens das Java 2 Platform Standard Edition Development Kit Version 1.5. Wenn Sie eine frühere Version verwenden, wird die WAR-Datei der Benutzeranwendung bei der Installation nicht richtig konfiguriert. Die Installation scheint erfolgreich zu verlaufen, Sie erhalten aber Fehlermeldungen, wenn Sie die Benutzeranwendung starten.

---

1. Sobald Sie die entsprechenden Installationsdateien erhalten haben, die in Tabelle 2-2 auf Seite 18 beschrieben werden, melden Sie sich an und öffnen Sie eine Terminal-Sitzung.
2. Starten Sie das Installationsprogramm für Ihre Plattform mit Java und gehen Sie wie folgt vor:

   ```
   java -jar IdmUserApp.jar -i console
   ```

3. Befolgen Sie die unter Kapitel 5, „Installieren der Benutzeranwendung auf JBoss“, auf Seite 59 für die grafische Benutzeroberfläche beschriebenen Schritte. Beachten Sie die Eingabeaufforderungen und geben Sie die Antworten in der Befehlszeile ein. Führen Sie die Schritte zum Importieren oder Erstellen des Master-Schlüssels aus.
4. Starten Sie das Dienstprogramm „ConfigUpdate“, um die Konfigurationsparameter für die Benutzeranwendung festzulegen. Geben Sie in der Befehlszeile `configupdate.sh` (Linux oder Solaris) oder `configupdate.bat` (Windows) ein und geben Sie die Werte, wie in Abschnitt A.1, „Benutzeranwendung - Konfiguration: Standardparameter“, auf Seite 157 beschrieben, ein.
5. Wenn Sie eine externe WAR-Datei für die Passwortverwaltung verwenden, kopieren Sie sie manuell in das Installationsverzeichnis und in das Bereitstellungsverzeichnis des Remote-JBoss-Servers, auf dem die externe Passwort-WAR ausgeführt wird.
6. Fahren Sie mit Kapitel 9, „Aufgaben nach Abschluss der Installation“, auf Seite 149 fort.

8.2 Installation der Benutzeranwendung mit einem einzigen Befehl

In diesem Abschnitt wird die Durchführung einer automatischen Installation beschrieben. Eine automatische Installation erfordert keine Benutzeraktion und kann Zeit einsparen, besonders, wenn die Installation auf mehreren Systemen erfolgt. Die automatische Installation wird unter Linux und Solaris unterstützt.

1. Rufen Sie die in Tabelle 2-2 auf Seite 18 beschriebenen Installationsdateien ab.
2. Melden Sie sich an und eröffnen Sie eine Terminalsitzung.
3. Suchen Sie die Identity Manager-Eigenschaftendatei `silent.properties`, die Teil der Installationsdateien ist. Wenn Sie von einer CD aus arbeiten, machen Sie eine lokale Kopie dieser Datei.
4. Bearbeiten Sie die `silent.properties`-Datei, sodass sie Ihre Installationsparameter und die Konfigurationsparameter der Benutzeranwendung zur Verfügung stellt.

   In der `silent.properties`-Datei finden Sie ein Beispiel für die einzelnen Installationsparameter. Die Installationsparameter entsprechen den Installationsparametern, die Sie bei der Installation der GUI oder der Konsolenschnittstelle angegeben haben.

   Eine Beschreibung der einzelnen Benutzeranwendungs-Konfigurationsparameter finden Sie in Tabelle 8-1. Die Benutzeranwendungs-Konfigurationsparameter sind identisch mit den Parametern, die Sie bei der Installation der GUI oder der Konsolenschnittstelle bzw. mit dem Dienstprogramm „ConfigUpdate“ einrichten können.
5. Starten Sie die automatische Installation wie folgt:

   ```
   java -jar IdmUserApp.jar -i silent -f / IhrVerzeichnispfad/
   silent.properties
   ```

   Geben Sie den vollständigen Pfad zur Datei `silent.properties` ein, falls sich die Datei in einem anderen Verzeichnis befindet als das Skript des Installationsprogramms. Das Skript entpackt die notwendigen Dateien in ein temporärer Verzeichnis und startet die automatische Installation.

Tabelle 8-1 *Benutzeranwendungs-Konfigurationsparameter für eine automatische Installation*

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
NOVL_CONFIG_LDAPHOST=	eDirectory-Verbindungseinstellungen: LDAP-Host. Geben Sie den Hostnamen oder die IP-Adresse des LDAP-Servers an.
NOVL_CONFIG_LDAPADMIN=	eDirectory-Verbindungseinstellungen: LDAP-Administrator. Geben Sie die Berechtigungsnachweise für den LDAP-Administrator an. Dieser Benutzer muss bereits vorhanden sein. Die Benutzeranwendung verwendet dieses Konto für eine administrative Verbindung zum Identitätsdepot. Dieser Wert ist mit dem Master-Schlüssel verschlüsselt.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
NOVL_CONFIG_LDAPADMINPASS=	eDirectory-Verbindungseinstellungen: LDAP-Administratorpasswort. Geben Sie das LDAP-Administratorpasswort an. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt.
NOVL_CONFIG_ROOTCONTAINERNAME=	eDirectory-DNs: Stammcontainer-DN. Geben Sie den eindeutigen LDAP-Namen des Stammcontainers an. Diese Angabe wird als Standard-Suchstamm der Entitätsdefinition verwendet, sofern in der Verzeichnisabstraktionsschicht kein Suchstamm angegeben wurde.
NOVL_CONFIG_PROVISIONROOT=	eDirectory-DNs: Bereitstellungstreiber-DN. Geben Sie den eindeutigen Namen für den Benutzeranwendungstreiber an. Wenn Ihr Treiber beispielsweise „UserApplicationDriver“ und der Treibersatz „myDriverSet“ ist und sich der Treibersatz in einem Kontext „o=myCompany“ befindet, geben Sie folgenden Wert ein: `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
NOVL_CONFIG_LOCKSMITH=	eDirectory-DNs: Benutzeranwendung - Administrator. Ein vorhandener Benutzer im Identitätsdepot mit den Rechten zum Ausführen von administrativen Tätigkeiten für den in der Benutzeranwendung angegebenen Benutzercontainer. Dieser Benutzer hat die Möglichkeit, über den Karteireiter *Administration* der Benutzeranwendung das Portal zu verwalten. Wenn der Benutzeranwendungsadministrator in iManager, Novell Designer für Identity Manager oder der Benutzeranwendung (Registerkarte *Anforderungen und Genehmigungen*) freigelegte Aufgaben zur Workflow-Administration bearbeitet, müssen Sie dem entsprechenden Administrator ausreichende Trustee-Rechte auf Objektinstanzen gewähren, die im Benutzeranwendungstreiber enthalten sind. Weitere Informationen finden Sie im *Administrationshandbuch zur Benutzeranwendung*. Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten *Administration* > *Sicherheit* der Benutzeranwendung geändert werden.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
NOVL_CONFIG_PROVLOCKSMITH=	eDirectory-DNs: Bereitstellungsanwendung - Administrator. Diese Rolle ist in der Bereitstellungsversion von Identity Manager verfügbar. Der Administrator für die Bereitstellungsanwendung kann die Funktionen des Bereitstellungs-Workflows über die Registerkarte *Bereitstellung* (in der Registerkarte *Administration*) verwalten. Auf diese Funktionen können die Benutzer über den Karteireiter *Anforderungen und Genehmigungen* der Benutzeranwendung zugreifen. Dieser Benutzer muss im Identitätsdepot vorhanden sein, bevor ihm die Rolle des Administrators für die Bereitstellungsanwendung zugewiesen werden kann. Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten *Administration* > *Sicherheit* der Benutzeranwendung geändert werden.
NOVL_CONFIG_ROLECONTAINERDN=	Diese Rolle ist im rollenbasierten Bereitstellungsmodul für Novell Identity Manager verfügbar. Mit dieser Rolle können Mitglieder alle Rollen erstellen, entfernen oder modifizieren und Benutzern, Gruppen oder Containern Rollen zuweisen oder entziehen. Außerdem können die Rollenmitglieder damit einen Bericht für einen beliebigen Benutzer ausführen. Standardmäßig wird diese Rolle dem Benutzeranwendungsadministrator zugewiesen. Sie können diese Zuweisung nach dem Bereitstellen der Benutzeranwendung über die Seite *Rollen* > *Rollenzuweisungen* in der Benutzeranwendung ändern.
NOVL_CONFIG_COMPLIANCECONTAINERDN	Der Konformitätsmoduladministrator ist eine Systemrolle, die es Mitgliedern ermöglicht, alle Funktionen der Registerkarte *Konformität* durchzuführen. Dieser Benutzer muss im Identitätsdepot vorhanden sein, damit ihm die Rolle des Konformitätsmoduladministrators zugewiesen werden kann.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
NOVL_CONFIG_USERCONTAINERDN=	Benutzeridentität für Metaverzeichnis: Benutzercontainer-DN. Geben Sie den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten Namen des Benutzercontainers an. Diese Angabe definiert den Suchbereich für Benutzer und Gruppen. Benutzer in diesem Container (und unterhalb) dürfen sich bei der Benutzeranwendung anmelden. **Wichtig:** Stellen Sie sicher, dass der bei der Installation des Benutzeranwendungstreibers angegebene Benutzeranwendungsadministrator in diesem Container vorhanden ist, wenn dieser Benutzer Workflows ausführen können soll.
NOVL_CONFIG_GROUPCONTAINERDN=	Benutzergruppen für Metaverzeichnis: Gruppencontainer-DN. Geben Sie den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten Namen des Gruppencontainers an. Wird von Entitätsdefinitionen innerhalb der Verzeichnisabstraktionsschicht verwendet.
NOVL_CONFIG_KEYSTOREPATH=	eDirectory-Zertifikate: Keystore-Pfad. Erforderlich. Geben Sie den vollständigen Pfad zur Keystore-Datei (`cacerts`) der JRE an, die der Anwendungsserver verwendet. Während der Installation der Benutzeranwendung wird die Keystore-Datei geändert. Unter Linux oder Solaris benötigt der Benutzer eine entsprechende Berechtigung zum Schreiben in diese Datei.
NOVL_CONFIG_KEYSTOREPASSWORD=	eDirectory-Zertifikate: Keystore-Passwort. Geben Sie das `cacerts`-Passwort an. Die Vorgabe ist `changeit`.
NOVL_CONFIG_SECUREADMINCONNECTION=	eDirectory-Verbindungseinstellungen: Sichere Admin-Verbindung. Erforderlich. Wählen Sie *True*, wenn die gesamte Kommunikation über das Admin-Konto über eine SSL-Verbindung erfolgen muss (diese Option kann die Leistung beeinträchtigen). Diese Einstellung ermöglicht, dass andere Vorgänge, für die kein SSL erforderlich ist, ohne SSL durchgeführt werden können. Wählen Sie *False*, wenn die Kommunikation über das Admin-Konto nicht über eine SSL-Verbindung erfolgen soll.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
NOVL_CONFIG_SECUREUSERCONNECTION=	eDirectory-Verbindungseinstellungen: Sichere Benutzerverbindung. Erforderlich. Wählen Sie *True*, wenn die gesamte Kommunikation über das Konto des angemeldeten Benutzers über eine SSL-Verbindung erfolgen muss (diese Option kann die Leistung stark beeinträchtigen). Diese Einstellung ermöglicht, dass andere Vorgänge, für die kein SSL erforderlich ist, ohne SSL durchgeführt werden können. Wählen Sie *False*, wenn die Kommunikation über das Benutzerkonto nicht über eine SSL-Verbindung erfolgen soll.
NOVL_CONFIG_SESSIONTIMEOUT=	Sonstige: Sitzungszeitüberschreitung. Erforderlich. Geben Sie für die Benutzeranwendung einen Zeitüberschreitungsintervall an.
NOVL_CONFIG_LDAPPLAINPORT=	eDirectory-Verbindungseinstellungen: Nicht sicherer LDAP-Port. Erforderlich. Geben Sie den nicht sicheren Port des LDAP-Servers an, z. B. Port 389.
NOVL_CONFIG_LDAPSECUREPORT=	eDirectory-Verbindungseinstellungen: Sicherer LDAP-Port. Erforderlich. Geben Sie den sicheren Port des LDAP-Servers an, z. B. Port 636.
NOVL_CONFIG_ANONYMOUS=	eDirectory-Verbindungseinstellungen: Öffentliches anonymes Konto verwenden. Erforderlich. Wählen Sie *True*, damit nicht angemeldete Benutzer auf das öffentliche anonyme LDAP-Konto zugreifen können. Wählen Sie *False*, um stattdessen NOVL_CONFIG_GUEST zu aktivieren.
NOVL_CONFIG_GUEST=	eDirectory-Verbindungseinstellungen: LDAP-Gast. Ermöglicht nicht angemeldeten Benutzern den Zugriff auf zulässige Portlets. Die Option *Öffentliches anonymes Konto verwenden* muss deaktiviert werden. Das Gast-Benutzer-Konto muss bereits im Identitätsdepot vorhanden sein. Aktivieren Sie zum Deaktivieren des Gast-Benutzers das Kontrollkästchen *Öffentliches anonymes Konto verwenden*.
NOVL_CONFIG_GUESTPASS=	eDirectory-Verbindungseinstellungen: LDAP-Gastpasswort.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
NOVL_CONFIG_EMAILNOTIFYHOST=	Email: Benachrichtigungsschablonen-Host-Token. Geben Sie den Anwendungsserver an, der die Identity Manager-Benutzeranwendung. Beispiel: `myapplication serverServer` Dieser Wert ersetzt das $HOST$-Token in Email-Schablonen. Die erstellte URL ist eine Verknüpfung zu Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen.
NOVL_CONFIG_EMAILNOTIFYPORT=	Email: Benachrichtigungsschablonen-Port-Token. Ersetzt das $PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungsaufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
NOVL_CONFIG_EMAILNOTIFYSECUREPORT=	Email: Token für den sicheren Port der Benachrichtigungsschablone. Ersetzt das $SECURE_PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden
NOVL_CONFIG_NOTFSMTPEMAILFROM=	Benachrichtigungs-SMTP-Email-Von. Erforderlich. Geben Sie Emails an, die von einem Benutzer in der Bereitstellungs-Email stammen.
NOVL_CONFIG_NOTFSMTPEMAILHOST=	Email: Benachrichtigungs-SMTP-Email-Host. Erforderlich. Geben Sie den SMTP-Email-Host für die Bereitstellungs-Email an. Dies kann eine IP-Adresse oder ein DNS-Name sein.
NOVL_CONFIG_USEEXTPWDWAR=	Passwortverwaltung: Externe WAR-Datei für Passwort verwenden. Wählen Sie *True*, falls Sie eine externe WAR-Datei für die Passwortverwaltung verwenden. Wenn Sie *True* angeben, müssen auch Werte für *NOVL_CONFIG_EXTPWDWARPTH* und *NOVL_CONFIG_EXTPWDWARRTNPATH* angegeben werden. Geben Sie *Falsch* an, um die interne Standardfunktion für die Passwortverwaltung zu verwenden.`/jsps/pwdmgt/ForgotPassword.jsp` (ohne http[s] am Anfang). Hierdurch wird der Benutzer nicht zu einer externen WAR-Datei, sondern zur in der Benutzeranwendung integrierten Funktionalität „Passwort vergessen“ umgeleitet.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
NOVL_CONFIG_EXTPWDWARPATH=	Passwortverwaltung: 'Passwort vergessen'-Link. Geben Sie die URL für die Seite „Passwort vergessen“ `ForgotPassword.jsp` in einer externen oder internen WAR-Datei für die Passwortverwaltung an. Alternativ können Sie auch die vorgegebene WAR-Datei für die Passwortverwaltung übernehmen. Weitere Informationen finden Sie in „Konfigurieren der externen Verwaltung „Passwort vergessen““ auf Seite 152.
NOVL_CONFIG_EXTPWDWARRTNPATH=	Passwortverwaltung: Link zurück zu 'Passwort vergessen'. Geben Sie den „Link zurück zu 'Passwort vergessen'“ an, den der Benutzer nach Durchführung eines „Passwort vergessen“-Vorgangs anklicken kann.
NOVL_CONFIG_FORGOTWEBSERVICEURL=	Passwortverwaltung: Webservice-URL zu „Passwort vergessen“. Dies ist die URL, die die externe WAR-Datei für „Passwort vergessen“ verwendet, um die Benutzeranwendung zum Durchführen von Kernfunktionen von „Passwort vergessen“ aufzurufen. Das Format der URL ist: `https://<idmhost>:<sslport>/<idm>/pwdmgt/service`
NOVL_CONFIG_USEROBJECTATTRIBUTE=	Benutzeridentität für Metaverzeichnis: Benutzerobjektklasse. Erforderlich. Die LDAP-Benutzerobjektklasse (in der Regel inetOrgPerson).
NOVL_CONFIG_LOGINATTRIBUTE=	Benutzeridentität für Metaverzeichnis: Anmeldeattribut. Erforderlich. Das LDAP-Attribut (z. B. CN), das den Anmeldenamen des Benutzers repräsentiert.
NOVL_CONFIG_NAMINGATTRIBUTE=	Benutzeridentität für Metaverzeichnis: Benennungsattribut. Erforderlich. Das als ID verwendete LDAP-Attribut beim Nachschlagen von Benutzern oder Gruppen. Dieses Attribut ist nicht identisch mit dem Anmeldeattribut, das nur für die Anmeldung, nicht aber bei der Suche nach Benutzern oder Gruppen verwendet wird.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
NOVL_CONFIG_USERMEMBERSHIPATTRIBUTE=	Benutzeridentität für Metaverzeichnis: Benutzermitgliedschaftsattribut. Optional. Erforderlich. Das LDAP-Attribut, das die Gruppenmitgliedschaft des Benutzers repräsentiert. Der Name darf keine Leerzeichen enthalten.
NOVL_CONFIG_GROUPOBJECTATTRIBUTE=	Benutzergruppen für Metaverzeichnis: Gruppenobjektklasse. Erforderlich. Die Objektklasse für die LDAP-Gruppen (in der Regel groupofNames).
NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE=	Benutzergruppen für Metaverzeichnis: Gruppenmitgliedschaftsattribut. Erforderlich. Geben Sie das Attribut an, das die Gruppenmitgliedschaft des Benutzers repräsentiert. Der Name darf keine Leerzeichen enthalten.
NOVL_CONFIG_USEDYNAMICGROUPS=	Benutzergruppen für Metaverzeichnis: Dynamische Gruppen verwenden. Erforderlich. Wählen Sie *True*, um dynamische Gruppen zu verwenden. Anderenfalls wählen Sie *False*.
NOVL_CONFIG_DYNAMICGROUPOBJECTCLASS=	Benutzergruppen für Metaverzeichnis: Klasse für dynamisches Gruppenobjekt. Erforderlich. Geben Sie die Objektklasse für die dynamische Gruppe an (in der Regel dynamicGroup).
NOVL_CONFIG_TRUSTEDSTOREPATH=	Speicher für Herkunftsverbürgungsschlüssel: Pfad für Herkunftsverbürgungsspeicher. Der Speicher für Herkunftsverbürgungsschlüssel enthält alle verbürgten Zertifikate der Signierer. Wurde kein Pfad angegeben, ruft die Benutzeranwendung den Pfad von der Systemeigenschaft `javax.net.ssl.trustStore` ab. Wurde kein Pfad angegeben, wird `jre/lib/security/cacerts` verwendet.
NOVL_CONFIG_TRUSTEDSTOREPASSWORD=	Speicher für Herkunftsverbürgungsschlüssel: Passwort für Herkunftsverbürgungsspeicher.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
NOVL_CONFIG_ICSLOGOUTENABLED=	Access Manager- und iChain-Einstellungen: Gleichzeitige Abmeldung aktiviert. Geben Sie *True* an, um die gleichzeitige Abmeldung von der Benutzeranwendung und entweder dem Novell Access Manager oder iChain zu aktivieren. Bei der Abmeldung leitet die Benutzeranwendung den Benutzer bei Vorhandensein des iChain- oder Novell Access Manager-Cookies zur ICS-Abmeldungsseite um. Wählen Sie *False*, um die gleichzeitige Abmeldung zu deaktivieren.
NOVL_CONFIG_ICSLOGOUTPAGE=	Access Manager- und iChain-Einstellungen: Seite 'Gleichzeitige Abmeldung'. Geben Sie die URL zur iChain- oder Novell Access Manager-Abmeldungsseite an, wobei die URL ein von iChain oder vom Novell Access Manager erwarteter Hostname ist. Wenn die ICS-Protokollierung aktiviert ist und sich ein Benutzer von der Benutzeranwendung abmeldet, wird der Benutzer auf diese Seite umgeleitet.
NOVL_CONFIG_EMAILNOTIFYPROTOCOL=	Email: Benachrichtigungsschablonen-Protokoll-Token. Bezieht sich auf ein nicht sicheres Protokoll, HTTP. Ersetzt das $PROTOCOL$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
NOVL_CONFIG_EMAILNOTIFYSECUREPROTOCOL=	Email: Token für den sicheren Port der Benachrichtigungsschablone.
NOVL_CONFIG_OCSPURI=	Sonstige: OCSP-URI. Wenn für die Client-Installation das OSCP (On-Line Certificate Status Protocol) verwendet wird, stellen Sie eine URI (Uniform Resource Identifier) bereit. Beispiel für das Format: http://hstport/ocspLocal. Die OCSP-URI aktualisiert den Status der verbürgten Zertifikate online.
NOVL_CONFIG_AUTHCONFIGPATH=	Sonstige: Konfigurationspfad für Autorisierung. Der vollständig qualifizierte Name der Konfigurationsdatei für die Autorisierung.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
NOVL_CONFIG_CREATEDIRECTORYINDEX	Sonstiges: eDirectory-Index erstellen Geben Sie „true“ an, wenn das automatische Installationsprogramm Indizes für die Attribute „manager“, „ismanager“ und „srvprvUUID“ auf dem eDirectory-Server erstellen soll, der in NOVL_CONFIG_SERVERDN angegeben wurde. Wenn dieser Parameter auf „true“ gesetzt ist, kann NOVL_CONFIG_REMOVEEDIRECTORYINDEX nicht auf „true“ gesetzt werden. Zur Erzielung einer optimalen Leistung sollte die Erstellung des Index abgeschlossen sein. Die Indizes sollten sich im Online-Modus befinden, bevor Sie die Benutzeranwendung verfügbar machen.
NOVL_CONFIG_REMOVEDIRECTORYINDEX	Sonstiges: eDirectory-Index entfernen Geben Sie „true“ an, wenn das automatische Installationsprogramm Indizes vom Server entfernen soll, der in NOVL_CONFIG_SERVERDN angegeben wurde. Wenn dieser Parameter auf „true“ gesetzt ist, kann NOVL_CONFIG_CREATEEDIRECTORYINDEX nicht den Wert „true“ haben.
NOVL_CONFIG_SERVERDN	Sonstiges: Server-DN Geben Sie den eDirectory-Server an, auf dem Indizes erstellt oder entfernt werden sollen.
NOVL_CREATE_DB	Gibt an, wie die Datenbank erstellt werden soll. Zur Auswahl stehen: ◆ now - Erstellt die Datenbank sofort ◆ file - Schreibt die SQL-Ausgabe in eine Datei ◆ startup - Erstellt die Datenbank, wenn die Anwendung gestartet wird
NOVL_DATABASE_NEW	Gibt an, ob diese Datenbank neu oder bereits vorhanden ist. Geben Sie *Wahr* an, wenn es sich um eine neue Datenbank handelt. Geben Sie *Falsch* an, wenn es sich um eine vorhandene Datenbank handelt.

Name des Benutzeranwendungs-Parameters in der Datei „silent.properties“	Entsprechender Parametername in der Datei mit den Benutzeranwendungs-Konfigurationsparametern
NOVL_RBPM_SEC_ADMINDN	Sicherheitsadministrator. Diese Rolle bietet Mitgliedern die ganze Funktionspalette innerhalb der Sicherheitsdomäne. Der Sicherheitsadministrator kann für alle Objekte alle möglichen Aktionen innerhalb der Sicherheitsdomäne durchführen. Die Sicherheitsdomäne erlaubt es dem Sicherheitsadministrator, Zugriffsberechtigungen für alle Objekte in allen Domänen innerhalb des rollenbasierten Bereitstellungsmoduls zu konfigurieren. Der Sicherheitsadministrator kann Teams konfigurieren sowie Domänenadministratoren, beauftragte Administratoren und andere Sicherheitsadministratoren zuweisen.
NOVL_RBPM_RESOURCE_ADMINDN	Ressourcenadministrator. Diese Rolle bietet Mitgliedern die ganze Funktionspalette innerhalb der Ressourcendomäne. Der Ressourcenadministrator kann für alle Objekte alle möglichen Aktionen innerhalb der Ressourcendomäne durchführen.
NOVL_RBPM_CONFIG_ADMINDN	Diese Rolle bietet Mitgliedern die ganze Funktionspalette innerhalb der Konfigurationsdomäne. Der RBPM-Konfigurationsadministrator kann für alle Objekte alle möglichen Aktionen innerhalb der Konfigurationsdomäne durchführen. Der RBPM-Konfigurationsadministrator steuert den Zugriff auf Navigationselemente innerhalb des rollenbasierten Bereitstellungsmoduls. Außerdem konfiguriert der RBPM-Konfigurationsadministrator den Delegierungs- und Vertretungsservice, die Bereitstellungsbenutzerschnittstelle und die Workflow-Engine.
RUN_LDAPCONFIG=	Gibt an, ob Sie die LDAP-Einstellungen jetzt oder später konfigurieren möchten. Gültige Werte: ◆ Now - Führt die LDAP-Konfiguration sofort aus, indem die WAR mit den angegebenen LDAP-Konfigurationseinstellungen gefüllt wird. ◆ Later - Installiert die Benutzeranwendungsdateien, ohne die LDAP-Einstellungen zu konfigurieren.

8.3 Ausführen des JBossPostgreSQL-Dienstprogramms im Automatik- oder im Konsolenmodus

Sie können das JBossPostgreSQL-Dienstprogramm im Automatik- oder im Konsolenmodus ausführen. Vor der Ausführung des Dienstprogramms im Automatikmodus müssen Sie die Eigenschaftendatei für das JBossPostgreSQL-Dienstprogramm bearbeiten. Wenn Sie die Eigenschaftendatei bearbeitet haben, starten Sie das Dienstprogramm mit diesem Befehl:

```
JBossPostgreSQL -i silent -f <path to the properties file>
```

Beispiel:

```
JBossPostgreSQL -i silent -f /home/jdoe/idm-install-files/silent.properties
```

Dies sind die Eigenschaften für eine automatische Installation von JBossPostgreSQL:

Tabelle 8-2 *JBossPostgreSQL-Konfigurationseigenschaften*

Eigenschaft	Beschreibung
USER_INSTALL_DIR	Pfad, in den Sie JBoss und die JRE installieren möchten. Erforderlich für die Installation von JBoss; anderenfalls kein Eintrag erforderlich.
NOVL_DB_NAME	Name der zu verwendenden Datenbank. Der Standarddatenbankname lautet „idmuserappdb“. Erforderlich für die Installation von PostgreSQL. Wenn Sie PostgreSQL nicht installieren, wird dieser Wert ignoriert.
NOVL_DB_PASSWORD	Root-Passwort für Datenbank. Erforderlich für die Installation von PostgreSQL. Wenn Sie PostgreSQL nicht installieren, wird dieser Wert ignoriert.
NOVL_DB_PASSWORD_CONFIRM	Bestätigt das Root-Passwort der Datenbank. Erforderlich für die Installation von PostgreSQL. Wenn Sie PostgreSQL nicht installieren, wird dieser Wert ignoriert.

CHOSEN_INSTALL_FEATURE_LIST	Zu installierende Installationssets.
	
	Erforderlich. Sie können sowohl JBoss als auch PostgreSQL auswählen oder nur eines dieser Produkte installieren.
	
	Beispiele:
	
	`CHOSEN_INSTALL_FEATURE_LIST=JBoss, PostgreSQL`
	
	`CHOSEN_INSTALL_FEATURE_LIST=JBoss,""`

Eigenschaft	Beschreibung
NOVL_POSTGRESQL_INSTALL_DIR	Name des Installationsverzeichnisses für PostgreSQL. Erforderlich für die Installation von PostgreSQL. Diese Eigenschaft wird ignoriert, wenn CHOSEN_INSTALL_FEATURE_LIST nicht PostgreSQL enthält.
START_DB	Gibt an, ob das Installationsprogramm die Datenbank während der Installation startet. Weisen Sie den Wert „Start“ zu, wenn das Installationsprogramm die Datenbank starten soll. Lassen Sie diese Eigenschaft anderenfalls leer. Optional.

8.4 Ausführen des RIS-Installationsprogramms im Automatik- oder im Konsolenmodus

Diese Version wird mit einem separaten Installationsprogramm ausgeliefert, mit dem Sie Rest Information Services (RIS) konfigurieren können. Dies stellt eine Möglichkeit dar, die RIS.war-Datei zu konfigurieren, die REST-Ressourcen unterstützt. Die über RIS freigelegten REST-Ressourcen führen SOAP-Aufrufe zum Sammeln von Informationen zu verschiedenen RBPM-Systemen durch.

Sie können das RIS-Installationsprogramm im Konsolen- oder im Automatikmodus ausführen. Vor der Ausführung des Installationsprogramms müssen Sie die Eigenschaftendatei für das RIS-Installationsprogramm bearbeiten. Wenn Sie die Eigenschaftendatei bearbeitet haben, starten Sie das Dienstprogramm mit diesem Befehl:

```
RisUpdateWar -i silent -f <path to the properties file>
```

Beispiel:

```
RisUpdateWar -i silent -f /home/jdoe/idm-install-files/silent.properties
```

Das Installationsprogramm benötigt die folgenden Informationen:

- Wo sich die RIS.war-Datei befindet
- Auf welchem Port die Benutzeranwendung zur Ausführung konfiguriert ist
- Welcher Kontext für die Benutzeranwendung definiert wurde
- Auf welchem Host die RIS.war-Datei bereitgestellt wird

Dies sind die Eigenschaften für eine RIS-Installation:

Tabelle 8-3 *RIS-Konfigurationseigenschaften*

Eigenschaft	Beschreibung
NOVL_INSTALL_HOST	Name des Hosts, auf dem die RIS.war-Datei bereitgestellt wird. Dieser Name darf nicht „localhost“ sein. Erforderlich.
NOVL_USERAPP_PORT	Port, auf dem die RBPM-Benutzeranwendung zur Ausführung konfiguriert ist. Erforderlich.
NOVL_CONTEXT_NAME	Kontextname für die Benutzeranwendung. Erforderlich.
RIS_INSTALL_DIRECTORY	Verzeichnis, in dem sich die RIS.war-Datei befindet. Erforderlich.
RIS_WAR_FILE	Name der RIS.war-Datei. Ändern Sie nicht diesen Wert.
RIS_INSTALL_LOG	Name der Protokolldatei für das Installationsprogramm. Sie können der Datei einen beliebigen Namen geben. Das Installationsprogramm schreibt die Datei an den in der Eigenschaft RIS_INSTALL_DIR angegebenen Speicherort. Wenn Sie diese Eigenschaft leer lassen, lautet die Standard-Protokolldatei „RIS-Install.log“. Optional.

Aufgaben nach Abschluss der Installation

9

In diesem Abschnitt werden die nach der Installation durchzuführenden Aufgaben erläutert. Es werden u. a. folgende Themen erläutert:

- Abschnitt 9.1, „Aufzeichnen des Master-Schlüssels“, auf Seite 149
- Abschnitt 9.2, „Konfiguration der Benutzeranwendung“, auf Seite 149
- Abschnitt 9.3, „Konfiguration von eDirectory“, auf Seite 150
- Abschnitt 9.4, „Neukonfiguration der Benutzeranwendungs-WAR-Datei nach der Installation“, auf Seite 152
- Abschnitt 9.5, „Konfigurieren der externen Verwaltung „Passwort vergessen““, auf Seite 152
- Abschnitt 9.6, „Aktualisierung der Einstellungen für „Passwort vergessen““, auf Seite 154
- Abschnitt 9.7, „Sicherheitsüberlegungen“, auf Seite 154
- Abschnitt 9.8, „Erhöhen der IDM Java-Heap-Größe“, auf Seite 154
- Abschnitt 9.9, „Fehlersuche“, auf Seite 155

9.1 Aufzeichnen des Master-Schlüssels

Kopieren Sie direkt nach der Installation den verschlüsselten Master-Schlüssel und speichern Sie ihn an einem sicheren Ort.

1. Öffnen Sie die Datei `master-key.txt`, die sich im Installationsverzeichnis befindet.
2. Kopieren Sie den verschlüsselten Master-Schlüssel an einen sicheren Speicherort, auf den Sie bei einem Systemfehler zugreifen können.

Warnung: Bewahren Sie immer eine Kopie des verschlüsselten Master-Schlüssels auf. Der verschlüsselte Master-Schlüssel wird benötigt, um Zugriff auf verschlüsselte Daten zu erlangen, falls der Master-Schlüssel z. B. durch einen Gerätefehler verloren geht.

Erfolgt die Installation auf dem ersten Mitglied eines Clusters, müssen Sie diesen verschlüsselten Master-Schlüssel verwenden, wenn Sie die Benutzeranwendung auf anderen Cluster-Mitgliedern installieren.

9.2 Konfiguration der Benutzeranwendung

Anleitungen zur Konfiguration der Identity Manager-Benutzeranwendung und dem Rollensubsystem nach der Installation finden Sie in folgenden Quellen:

- Im *Administrationshandbuch zum rollenbasierten Bereitstellungsmodul für Novell IDM* im Abschnitt zur Konfiguration der Benutzeranwendungsumgebung
- Im *Designhandbuch zum rollenbasierten Bereitstellungsmodul für Novell IDM*

9.2.1 Einrichten der Protokollierung

Befolgen Sie zum Konfigurieren der Protokollierung die Anweisungen im Abschnitt „Setting Up Logging" (Protokollierung einrichten) im Benutzeranwendung: Administrationshandbuch (http://www.novell.com/documentation/idm40/index.html).

9.3 Konfiguration von eDirectory

- Abschnitt 9.3.1, „Erstellen von Indizes in eDirectory", auf Seite 150
- Abschnitt 9.3.2, „Installieren und Konfigurieren der SAML-Beglaubigungsmethode", auf Seite 150

9.3.1 Erstellen von Indizes in eDirectory

Um die Leistung der Benutzeranwendung zu verbessern, sollte der Administrator von eDirectory Indizes für die Attribute „manager", „ismanager" und „srvprvUUID" erstellen. Sind für diese Attribute keine Indizes vorhanden, kann dies insbesondere in einer Cluster-Umgebung eine eingeschränkte Leistung zur Folge haben.

Diese Indizes können automatisch während der Installation erstellt werden, wenn Sie *Index für eDirectory erstellen* auf der Registerkarte *Erweitert* des Teilfensters „Benutzeranwendung - Konfiguration" auswählen (beschrieben in Tabelle A-2 auf Seite 160). Alternativ erhalten Sie im *Novell eDirectory-Administrationshandbuch* (http://www.novell.com/documentation) weitere Anweisungen zur Verwendung des Index-Managers zum Erstellen von Indizes.

9.3.2 Installieren und Konfigurieren der SAML-Beglaubigungsmethode

Diese Konfiguration ist nur dann erforderlich, wenn Sie die SAML-Beglaubigungsmethode verwenden möchten, jedoch nicht den Access Manager verwenden. Wenn Sie den Access Manager verwenden, enthält Ihre eDirectory-Baumstruktur bereits die Methode. Das Verfahren umfasst folgende Schritte:

- ❑ Installieren der SAML-Methode in Ihrer eDirectory-Baumstruktur
- ❑ Bearbeiten der eDirectory-Attribute mithilfe von iManager

Installieren der SAML-Methode in Ihrer eDirectory-Baumstruktur

1. Suchen Sie im `.iso`-Image die Datei `nmassaml.zip` und entpacken Sie sie.
2. Installieren Sie die SAML-Methode in Ihre eDirectory-Baumstruktur.
   - **2a** Erweitern Sie das in `authsaml.sch` gespeicherte Schema.

     Im folgenden Beispiel wird die Durchführung unter Linux gezeigt:

     ```
     ndssch -h <edir_ip> <edir_admin> authsaml.sch
     ```
   - **2b** Installieren Sie die SAML-Methode.

     Im folgenden Beispiel wird die Durchführung unter Linux gezeigt:

     ```
     nmasinst   -addmethod <edir_admin> <tree> ./config.txt
     ```

Bearbeiten der eDirectory-Attribute

1. Öffnen Sie iManager und wechseln Sie zu *Rollen und Aufgaben* > *Verzeichnisadministration* > *Objekt erstellen*.
2. Wählen Sie *Alle Objektklassen anzeigen*.
3. Erstellen Sie ein neues Objekt der Klasse `authsamlAffiliate`.
4. Wählen Sie `authsamlAffiliate` und klicken Sie auf *OK*. (Sie können diesem Objekt einen beliebigen gültigen Namen geben.)
5. Wählen Sie das Containerobjekt *SAML Assertion.Authorized Login Methods.Security* in der Baumstruktur aus, um den Kontext anzugeben, und klicken Sie anschließend auf *OK*.
6. Sie müssen Attribute zum Klassenobjekt `authsamlAffiliate` hinzufügen.
   - **6a** Wechseln Sie zur iManager-Registerkarte *Objekte anzeigen* > *Durchsuchen* und suchen Sie Ihr neues affiliate-Objekt im Container „SAML Assertion.Authorized Login Methods.Security“.
   - **6b** Wählen Sie das neue affiliate-Objekt und wählen Sie anschließend *Objekt ändern* aus.
   - **6c** Fügen Sie ein *authsamlProviderID*-Attribut zum neuen affiliate-Objekt hinzu. Dieses Attribut dient der Übereinstimmung einer Assertion mit ihrem Partner. Der Inhalt dieses Attributs muss exakt mit dem Ausstellerattribut übereinstimmen, das von der SAML-Assertion gesendet wurde.
   - **6d** Klicken Sie auf *OK*.
   - **6e** Fügen Sie die Attribute *authsamlValidBefore* und *authsamlValidAfter* zum affiliate-Objekt hinzu. Diese Attribute definieren die Zeit in Sekunden um ein *IssueInstant* in einer Assertion, wenn die Assertion als gültig angesehen wird. Der übliche Standardwert ist 180 Sekunden.
   - **6f** Klicken Sie auf *OK*.
7. Wählen Sie den Sicherheitscontainer und anschließend *Objekt erstellen* aus, um einen *Herkunftsverbürgungscontainer* in Ihrem Sicherheitscontainer zu erstellen.
8. Erstellen Sie ein *Herkunftsverbürgung*sobjekt im Herkunftsverbürgungscontainer.
   - **8a** Kehren Sie zurück zu *Rollen und Aufgaben* > *Verzeichnisadministration* und wählen Sie anschließend *Objekt erstellen*.
   - **8b** Wählen Sie erneut *Alle Objektklassen anzeigen*.
   - **8c** So erstellen Sie ein *Herkunftsverbürgung*sobjekt für das Zertifikat, das Ihr Partner zum Signieren von Assertions verwendet. Sie benötigen hierzu eine verschlüsselte Kopie des Zertifikats.
   - **8d** Erstellen Sie neue Herkunftsverbürgungsobjekte für jedes Zertifikat in der Kette der unterzeichnenden Zertifikate bis zum Stamm-CA-Zertifikat.
   - **8e** Legen Sie den Kontext auf den zuvor erstellen Herkunftsverbürgungs-Container fest und klicken Sie anschließend auf *OK*.
9. Kehren Sie zum Objekt-Viewer zurück.
10. Fügen Sie ein *authsamlTrustedCertDN*-Attribut zum affiliate-Objekt hinzu und klicken Sie anschließend auf *OK*.

Dieses Attribut sollte auf das „Herkunftsverbürgungsobjekt“ für das unterzeichnende Zertifikat zeigen, das Sie im vorherigen Schritt erstellt haben. (Alle Assertions für den Partner müssen von Zertifikaten unterzeichnet werden, auf die dieses Attribut zeigt, sonst werden sie abgewiesen.)

11 Fügen Sie ein *authsamlCertContainerDN*-Attribut zum affiliate-Objekt hinzu und klicken Sie anschließend auf *OK*.

Dieses Attribut sollte auf den „Herkunftsverbürgungscontainer“ zeigen, den Sie bereits erstellt haben. (Dieses Attribut dient zur Überprüfung der Zertifikatskette des unterzeichnenden Zertifikats.)

9.4 Neukonfiguration der Benutzeranwendungs-WAR-Datei nach der Installation

Zum Aktualisieren Ihrer WAR-Datei können Sie das Dienstprogramm „ConfigUpdate“ folgendermaßen ausführen:

1 Führen Sie das Dienstprogramm „ConfigUpdate“ im Installationsverzeichnis der Benutzeranwendung aus, indem Sie `configupdate.sh` oder `configupdate.bat` ausführen. Dadurch können Sie die WAR-Datei im Installationsverzeichnis aktualisieren.

Weitere Informationen zu den Parametern des Dienstprogramms „ConfigUpdate“ finden Sie unter Abschnitt A.1, „Benutzeranwendung - Konfiguration: Standardparameter“, auf Seite 157, Tabelle 8-1 auf Seite 134.

2 Stellen Sie die neue WAR-Datei auf Ihrem Anwendungsserver bereit.

Verlagern Sie bei WebLogic und WebSphere die WAR-Datei auf den Anwendungsserver. Bei einem JBoss-Einzelserver werden die Änderungen auf die bereitgestellte WAR-Datei angewendet. Wenn Sie einen JBoss-Cluster ausführen, muss die WAR-Datei auf jedem JBoss-Server im Cluster aktualisiert werden.

9.5 Konfigurieren der externen Verwaltung „Passwort vergessen“

Geben Sie für den Konfigurationsparameter *'Passwort vergessen'-Link* den Standort einer WAR-Datei mit der Funktionalität „Passwort vergessen“ an. Hierbei kann es sich um eine externe oder interne WAR-Datei handeln.

- Abschnitt 9.5.1, „Angabe einer externen WAR-Datei für die Verwaltung von „Passwort vergessen““, auf Seite 153
- Abschnitt 9.5.2, „Angeben einer internen Passwort-WAR-Datei“, auf Seite 153
- Abschnitt 9.5.3, „Testen der externen WAR-Konfiguration für „Passwort vergessen““, auf Seite 153
- Abschnitt 9.5.4, „Konfiguration der SSL-Kommunikation zwischen JBoss-Servern“, auf Seite 154

9.5.1 Angabe einer externen WAR-Datei für die Verwaltung von „Passwort vergessen“

1. Sie können die externe WAR-Datei während des Installationsvorgangs oder über das Dienstprogramm „ConfigUpdate“ angeben.
2. Aktivieren Sie in den Konfigurationsparametern der Benutzeranwendung das Kontrollkästchen *Externe WAR-Datei für Passwort verwenden*.
3. Geben Sie für den Konfigurationsparameter *'Passwort vergessen'-Link* den Speicherort der externen Passwort-WAR-Datei an.

   Nehmen Sie den Host und den Port auf, z. B. `http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp`. Eine externe Passwort-WAR kann sich außerhalb der schützenden Firewall der Benutzeranwendung befinden.
4. Geben Sie für den *Link zurück zu 'Passwort vergessen'* den Link an, der angezeigt wird, wenn der Benutzer die Prozedur „Passwort vergessen“ abgeschlossen hat. Wenn der Benutzer auf diesen Link klickt, wird er auf den angegebenen Link umgeleitet.
5. Geben Sie für die *Webservice-URL zu 'Passwort vergessen'* die URL für den Webservice an, die die externe WAR-Datei für „Passwort vergessen“ verwendet, um die Benutzeranwendung aufzurufen. Das Format der URL ist: `https://<idmhost>:<sslport>/<idm>/pwdmgt/service`.

   Der Link zurück zu 'Passwort vergessen' muss SSL verwenden, sodass eine sichere Web-Service-Kommunikation mit der Benutzeranwendung gewährleistet ist. Siehe auch Abschnitt 9.5.4, „Konfiguration der SSL-Kommunikation zwischen JBoss-Servern“, auf Seite 154.
6. Kopieren Sie `ExternalPwd.war` in den Bereitstellungsordner des Remote-JBoss-Servers, auf dem die Funktionalität der externen Passwort-WAR ausgeführt wird.

9.5.2 Angeben einer internen Passwort-WAR-Datei

1. Aktivieren Sie in den Konfigurationsparametern der Benutzeranwendung nicht das Kontrollkästchen *Externe WAR-Datei für Passwort verwenden*.
2. Übernehmen Sie den vorgegebenen Speicherort unter *'Passwort vergessen'-Link* oder geben Sie eine URL zu einer anderen Passwort-WAR an.
3. Bestätigen Sie den vorgegebenen Wert für *Link zurück zu 'Passwort vergessen'*.

9.5.3 Testen der externen WAR-Konfiguration für „Passwort vergessen“

Wenn Sie eine externe Passwort-WAR verwenden und die „Passwort vergessen“-Funktion testen möchten, können Sie wie folgt auf sie zugreifen:

- Direkt, in einem Browser. Rufen Sie die Seite „Passwort vergessen“ in der externen Passwort-WAR-Datei auf, z. B. `http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp`.
- Klicken Sie auf der Anmeldeseite der Benutzeranwendung auf den Link *Passwort vergessen*.

9.5.4 Konfiguration der SSL-Kommunikation zwischen JBoss-Servern

Wenn Sie während der Installation *Externe WAR-Datei für Passwort verwenden* in der Benutzeranwendungskonfigurationsdatei auswählen, müssen Sie die SSL-Kommunikation zwischen den JBoss-Servern konfigurieren, auf denen die Benutzeranwendungs-WAR-Datei und die externe Verwaltungs-WAR-Datei für „Passwort vergessen“ bereitgestellt werden. Eine Anleitung hierzu finden Sie in der JBoss-Dokumentation.

9.6 Aktualisierung der Einstellungen für „Passwort vergessen“

Nach der Installation können Sie die Werte für *'Passwort vergessen'-Link*, *Link zurück zu 'Passwort vergessen'* und *Webservice-URL zu 'Passwort vergessen'* ändern. über das Dienstprogramm „ConfigUpdate“ oder die Benutzeranwendung geändert werden.

Verwendung des Dienstprogramms „ConfigUpdate“. Wechseln Sie in der Befehlszeile zum Installationsverzeichnis und geben Sie `configupdate.sh` (Linux oder Solaris) bzw. `configupdate.bat` (Windows) ein. Wenn Sie eine externe WAR-Datei für die Passwortverwaltung erstellen oder bearbeiten, müssen Sie die WAR-Datei manuell umbenennen, bevor Sie sie auf den Remote-JBoss-Server kopieren.

Verwendung der Benutzeranwendung. Melden Sie sich als Administrator der Benutzeranwendung an und wechseln Sie zu *Administration* > *Anwendungskonfiguration* > *Passwortmodul - Setup* > *Anmeldung*. Bearbeiten Sie folgende Felder:

- *'Passwort vergessen'-Link* (z. B. `http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp`)
- *Link zurück zu 'Passwort vergessen'* (z. B. `http://localhost/IDMProv`)
- *Webservice-URL für 'Passwort vergessen'* (z. B. `https://<idmhost>:<sslport>/<idm>/pwdmgt/service`)

9.7 Sicherheitsüberlegungen

Während des Installationsvorgangs legt das Installationsprogramm Protokolldateien im Installationsverzeichnis ab. Diese Dateien enthalten Informationen über Ihre Konfiguration. Sie können diese Dateien löschen oder an einem sicheren Speicherort aufbewahren, nachdem Ihre Umgebung konfiguriert wurde.

Während des Installationsvorgangs können Sie angeben, dass das Datenbankschema in eine Datei geschrieben werden soll. Da diese Datei beschreibende Informationen über Ihre Datenbank enthält, sollten Sie sie nach Abschluss der Installation an einem sicheren Speicherort aufbewahren.

9.8 Erhöhen der IDM Java-Heap-Größe

In einer Enterprise-Umgebung benötigen der Rollen- und Ressourcen-Service-Treiber mehr maximalen Java-Heap als die in IDM definierte Standardmenge. Es sollte die maximale Größe eines Java-Heap von 256 MB verwendet werden, um OutOfMemoryError-Bedingungen zu vermeiden.

Die Größe des Java-Heaps kann über iManager unter den sonstigen Einstellungen der Treibersatzeigenschaften oder durch Einstellen der Umgebungsvariablen DHOST_JVM_INITIAL_HEAP und DHOST_JVM_MAX_HEAP angegeben werden. Weitere Informationen zum Konfigurieren der Java VM-Optionen finden Sie im Identity Manager Common Driver Administration Guide (http://www.novell.com/documentation/idm40/idm_common_driver/index.html?page=/documentation/idm40/idm_common_driver/data/front.html) .

9.9 Fehlersuche

Ein Mitarbeiter von Novell unterstützt Sie bei der Behebung von Einrichtungs- und Konfigurationsproblemen. Unterdessen finden Sie in diesem Abschnitt einige Lösungsansätze zur Behebung von Problemen.

Problem	Empfohlene Vorgehensweise

Sie möchten die Benutzeranwendungs-Konfigurationseinstellungen ändern, die Sie während der Installation vorgenommen haben. Hierzu gehören folgende Konfigurationseinstellungen:
◆ Identitätsdepot-Verbindungen und -Zertifikate
◆ Email-Einstellungen
◆ Benutzeridentität für Metaverzeichnis, Benutzergruppen
◆ Access Manager- oder iChain-Einstellungen
	Das Dienstprogramm für die Konfiguration kann unabhängig vom Installationsprogramm ausgeführt werden.
	Führen Sie unter Linux und Solaris im Installationsverzeichnis (standardmäßig `\opt\novell\idm`) den folgenden Befehl aus:
	`configupdate.sh`
	Führen Sie unter Windows im Installationsverzeichnis (standardmäßig `c:\opt\novell\idm`) den folgenden Befehl aus:
	`configupdate.bat`

Beim Start des Anwendungsserver werden Ausnahmen sowie die Protokollmeldung `port 8180 already in use` ausgegeben.	Schließen Sie alle Instanzen von Tomcat (oder anderer Server-Software), die möglicherweise bereits laufen. Wenn Sie den Anwendungsserver neu konfigurieren und einen anderen Port als Port 8180 festlegen möchten, müssen Sie die `config`-Einstellungen für den Benutzeranwendungstreiber bearbeiten.
Beim Start des Anwendungsservers wird angezeigt, dass keine verbürgten Zertifikate gefunden wurden.	Stellen Sie sicher, dass Sie den Anwendungsserver mithilfe des JDK starten, das bei der Installation der Benutzeranwendung angegeben wurde.
Sie können sich nicht auf der Seite „Portaladministration“ anmelden.	Stellen Sie sicher, dass ein Konto für den Benutzeranwendungsadministrator vorhanden ist. Verwechseln Sie dieses Konto nicht mit Ihrem iManager-Administratorkonto. Dies sind zwei unterschiedliche Administratorobjekte (oder sollten es sein).
Sie können sich als Administrator anmelden, aber keine neuen Benutzer erstellen.	Der Administrator der Benutzeranwendung muss ein Trustee des Containers der obersten Ebene sein und über Supervisor-Rechte verfügen. Zur Überbrückung können Sie die Rechte des Administrators der Benutzeranwendung mit denen des LDAP-Administrators gleichsetzen (mithilfe von iManager).

Problem	Empfohlene Vorgehensweise
Beim Starten des Anwendungsservers treten Keystore-Fehler auf.	Ihr Anwendungsserver verwendet nicht das bei der Installation der Benutzeranwendung angegebene JDK. Importieren Sie die Zertifikatsdatei mithilfe des Befehls `keytool`: `keytool -import -trustcacerts -alias aliasName -file certFile -keystore ..\lib\security\cacerts -storepass changeit` ◆ Ersetzen Sie *aliasName* durch einen beliebigen eindeutigen Namen für dieses Zertifikat. ◆ Ersetzen Sie *certFile* durch den vollständigen Pfad und Namen der Zertifikatsdatei. ◆ Das Keystore-Standardpasswort lautet `changeit` (falls Sie ein anderes Passwort festgelegt haben, geben Sie es an).

Es wurde keine Email-Benachrichtigung gesendet.	Führen Sie das Dienstprogramm „ConfigUpdate“ aus, um zu überprüfen, ob Sie Werte für die Benutzeranwendungs-Konfigurationsparameter „Email-Von“ und „Email-Host“ angegeben haben.
	
	Führen Sie unter Linux und Solaris im Installationsverzeichnis (standardmäßig `\opt\novell\idm`) den folgenden Befehl aus:
	
	`configupdate.sh`
	
	Führen Sie unter Windows im Installationsverzeichnis (standardmäßig `c:\opt\novell\idm`) den folgenden Befehl aus:
	
	`configupdate.bat`

IDM Benutzeranwendung - Konfigurationsreferenz

A

In diesem Abschnitt werden die Optionen beschrieben, mit denen Werte während der Benutzeranwendungsinstallation oder einer Konfigurationsaktualisierung übergeben werden.

- Abschnitt A.1, „Benutzeranwendung - Konfiguration: Standardparameter“, auf Seite 157
- Abschnitt A.2, „Konfiguration der Benutzeranwendung: Alle Parameter“, auf Seite 160

A.1 Benutzeranwendung - Konfiguration: Standardparameter

Abbildung A-1 *Standardoptionen für die Konfiguration der Benutzeranwendung*

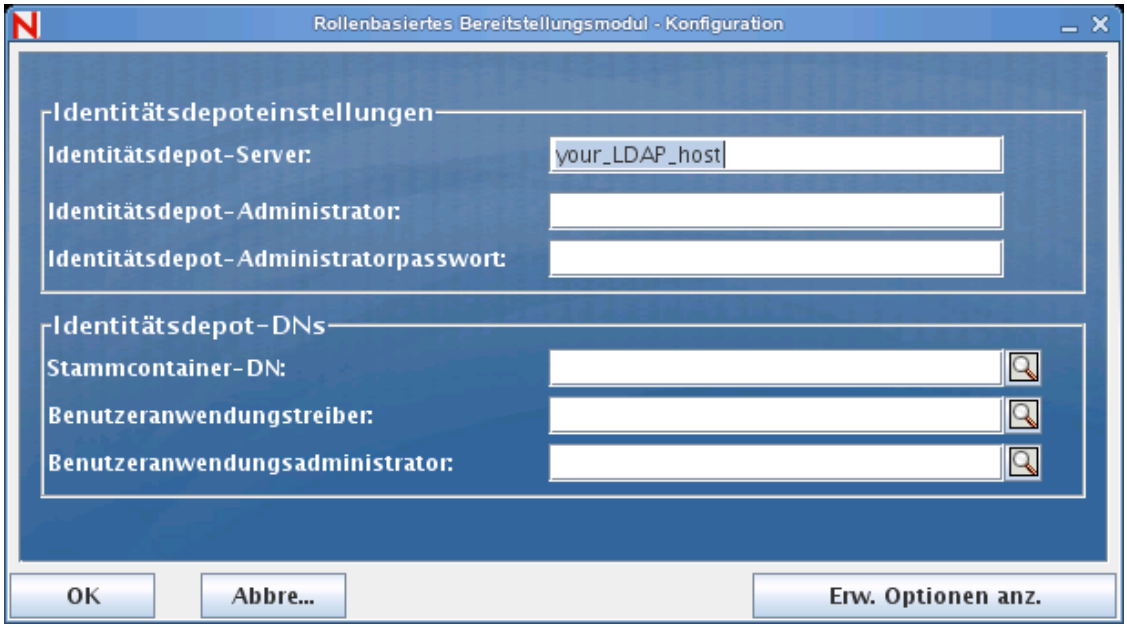


Tabelle A-1 *Standardoptionen für die Konfiguration der Benutzeranwendung*

Einstellungstyp	Option	Beschreibung
Identitätsdepot-einstellungen	*Identitätsdepot-Server*	Erforderlich. Geben Sie den Hostnamen oder die IP-Adresse sowie den sicheren Port des LDAP-Servers an. Beispiel: `myLDAPhost`
	Identitätsdepot-Administrator	Erforderlich. Geben Sie die Berechtigungsnachweise für den LDAP-Administrator an. Dieser Benutzer muss bereits vorhanden sein. Die Benutzeranwendung verwendet dieses Konto für eine administrative Verbindung zum Identitätsdepot. Dieser Wert ist mit dem Master-Schlüssel verschlüsselt. Sie können das Dienstprogramm „ConfigUpdate“ zum Bearbeiten dieser Einstellung verwenden, solange Sie sie nicht über die Registerkarte „Administration“ der Benutzeranwendung geändert haben.
	Identitätsdepot-Administrator-passwort	Erforderlich. Geben Sie das LDAP-Administratorpasswort an. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt. Sie können das Dienstprogramm „ConfigUpdate“ zum Bearbeiten dieser Einstellung verwenden, solange Sie sie nicht über die Registerkarte „Administration“ der Benutzeranwendung geändert haben.

Einstellungstyp	Option	Beschreibung
Identitätsdepot-DNs	*Stammcontainer-DN*	Erforderlich. Geben Sie den eindeutigen LDAP-Namen des Stammcontainers an. Diese Angabe wird als Standard-Suchstamm der Entitätsdefinition verwendet, sofern in der Verzeichnisabstraktionsschicht kein Suchstamm angegeben wurde.
	Benutzeranwendungstreiber-DN	Erforderlich. Geben Sie den eindeutigen Namen für den Benutzeranwendungstreiber an. Wenn Ihr Treiber beispielsweise „myDriverSet“ und der Treibersatz „myDriverSet“ ist und sich der Treibersatz in einem Kontext „o=myDriverSet“ befindet, geben Sie folgenden Wert ein: `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	Benutzeranwendungsadminis-trator	Erforderlich. Ein vorhandener Benutzer im Identitätsdepot mit den Rechten zum Ausführen von administrativen Tätigkeiten für den in der Benutzeranwendung angegebenen Benutzercontainer. Dieser Benutzer hat die Möglichkeit, über den Karteireiter *Administration* der Benutzeranwendung das Portal zu verwalten. Wenn der Benutzeranwendungsadministrator in iManager, Novell Designer für Identity Manager oder der Benutzeranwendung (Registerkarte *Anforderungen und Genehmigungen*) freigelegte Aufgaben zur Workflow-Administration bearbeitet, müssen Sie dem entsprechenden Administrator ausreichende Trustee-Rechte auf Objektinstanzen gewähren, die im Benutzeranwendungstreiber enthalten sind. Weitere Informationen finden Sie im *Administrationshandbuch zur Benutzeranwendung*. Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten *Administration* > *Sicherheit* der Benutzeranwendung geändert werden. Sie können diese Einstellung nicht über „ConfigUpdate“ ändern, wenn Sie den Anwendungsserver gestartet haben, auf dem die Benutzeranwendung installiert ist.
	Name des RBPM-Kontexts	Zeigt den Namen des aktuellen Kontexts an.
	RBPM Reporting-Administrator	Zeigt auf den Reporting-Administrator. Das Installationsprogramm setzt diesen Wert standardmäßig auf denselben Benutzer wie die anderen Sicherheitsfelder.

Hinweis: Die meisten Einstellungen in dieser Datei können nach der Installation bearbeitet werden. Führen Sie hierzu das `configupdate.sh`-Skript oder die Windows-Datei `configupdate.bat` aus, die sich im Installations-Unterverzeichnis befinden. Denken Sie daran, dass die Einstellungen in dieser Datei in einem Cluster für alle Cluster-Mitglieder identisch sein müssen.

A.2 Konfiguration der Benutzeranwendung: Alle Parameter

Diese Tabelle enthält die verfügbaren Konfigurationsparameter, wenn Sie auf *Erweiterte Optionen anzeigen* klicken.

Tabelle A-2 *Benutzeranwendung - Konfiguration: Alle Optionen*

Einstellungstyp	Option	Beschreibung
Identitätsdepot-einstellungen	*Identitätsdepot-Server*	Erforderlich. Geben Sie den Hostnamen oder die IP-Adresse des LDAP-Servers an. Beispiel: myLDAPhost
	LDAP-Port	Geben Sie den nicht sicheren Port des LDAP-Servers an. Beispiel: 389.
	Sicherer LDAP-Port	Geben Sie den sicheren Port des LDAP-Servers an. Beispiel: 636.
	Identitätsdepot-Administrator	Erforderlich. Geben Sie die Berechtigungsnachweise für den LDAP-Administrator an. Dieser Benutzer muss bereits vorhanden sein. Die Benutzeranwendung verwendet dieses Konto für eine administrative Verbindung zum Identitätsdepot. Dieser Wert ist mit dem Master-Schlüssel verschlüsselt.
	Identitätsdepot-Administrator-passwort	Erforderlich. Geben Sie das LDAP-Administratorpasswort an. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt.
	Öffentliches anonymes Konto verwenden	Ermöglicht nicht angemeldeten Benutzern den Zugriff auf das öffentliche anonyme LDAP-Konto.
	LDAP-Gast	Ermöglicht nicht angemeldeten Benutzern den Zugriff auf zulässige Portlets. Dieses Benutzerkonto muss bereits im Identitätsdepot vorhanden sein. Deaktivieren Sie das Kontrollkästchen *Öffentliches anonymes Konto verwenden*, um „LDAP-Gast“ zu aktivieren. Aktivieren Sie das Kontrollkästchen *Öffentliches anonymes Konto verwenden*, um „LDAP-Gast“ zu deaktivieren.
	LDAP-Gastpasswort	Geben Sie das LDAP-Gastpasswort an.
	Sichere Administrator-verbindung:	Wählen Sie diese Option aus, wenn die gesamte Kommunikation über das Admin-Konto über eine SSL-Verbindung erfolgen muss (diese Option kann die Leistung beeinträchtigen). Diese Einstellung ermöglicht, dass andere Vorgänge, für die kein SSL erforderlich ist, ohne SSL durchgeführt werden können.
	Sichere Benutzer-verbindung	Wählen Sie diese Option aus, wenn die gesamte Kommunikation über das Konto des angemeldeten Benutzers über eine SSL-Verbindung erfolgen muss (diese Option kann die Leistung stark beeinträchtigen). Diese Einstellung ermöglicht, dass andere Vorgänge, für die kein SSL erforderlich ist, ohne SSL durchgeführt werden können.

Einstellungstyp	Option	Beschreibung
Identitätsdepot-DNs	*Stammcontainer-DN*	Erforderlich. Geben Sie den eindeutigen LDAP-Namen des Stammcontainers an. Diese Angabe wird als Standard-Suchstamm der Entitätsdefinition verwendet, sofern in der Verzeichnisabstraktionsschicht kein Suchstamm angegeben wurde.
	Benutzeranwendungstreiber-DN	Erforderlich. Geben Sie den eindeutigen Namen für den Benutzeranwendungstreiber an. Wenn Ihr Treiber beispielsweise „UserApplicationDriver“ und der Treibersatz „myDriverSet“ ist und sich der Treibersatz in einem Kontext „o=myCompany“ befindet, geben Sie folgenden Wert ein: `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`
	Benutzeranwendungsadministrator	Erforderlich. Ein vorhandener Benutzer im Identitätsdepot mit den Rechten zum Ausführen von administrativen Tätigkeiten für den in der Benutzeranwendung angegebenen Benutzercontainer. Dieser Benutzer hat die Möglichkeit, über den Karteireiter *Administration* der Benutzeranwendung das Portal zu verwalten. Wenn der Benutzeranwendungsadministrator in iManager, Novell Designer für Identity Manager oder der Benutzeranwendung (Registerkarte *Anforderungen und Genehmigungen*) freigelegte Aufgaben zur Workflow-Administration bearbeitet, müssen Sie dem entsprechenden Administrator ausreichende Trustee-Rechte auf Objektinstanzen gewähren, die im Benutzeranwendungstreiber enthalten sind. Weitere Informationen finden Sie im *Benutzeranwendung: Administrationshandbuch*. Diese Zuweisung kann nach dem Bereitstellen der Benutzeranwendung über die Seiten *Administration* > *Sicherheit* der Benutzeranwendung geändert werden. Sie können diese Einstellung nicht über „ConfigUpdate“ ändern, wenn Sie den Anwendungsserver gestartet haben, auf dem die Benutzeranwendung installiert ist.
	Bereitstellungsadministrator	Der Bereitstellungsadministrator verwaltet die in der Benutzeranwendung verfügbaren Bereitstellungs-Workflow-Funktionen. Dieser Benutzer muss im Identitätsdepot vorhanden sein, bevor ihm die Rolle des Bereitstellungsadministrators zugewiesen werden kann. Sie können diese Zuweisung nach dem Bereitstellen der Benutzeranwendung über die Seite *Verwaltung* > *Administratorzuweisung* in der Benutzeranwendung ändern.

Einstellungstyp	Option	Beschreibung
	Konformitäts-administrator	Der Konformitätsadministrator ist eine Systemrolle, die es Mitgliedern ermöglicht, alle Funktionen auf der Registerkarte *Konformität* durchzuführen. Dieser Benutzer muss im Identitätsdepot vorhanden sein, damit ihm die Rolle des Konformitätsmoduladministrators zugewiesen werden kann. Während der Ausführung von „ConfigUpdate“ treten Änderungen an diesem Wert nur dann in Kraft, wenn kein gültiger Konformitätsadministrator zugewiesen wurde. Wenn ein gültiger Konformitätsadministrator existiert, werden Ihre Änderungen nicht gespeichert. Sie können diese Zuweisung nach dem Bereitstellen der Benutzeranwendung über die Seite *Verwaltung* > *Administratorzuweisung* in der Benutzeranwendung ändern.
	Rollen-administrator	Mit dieser Rolle können Mitglieder alle Rollen erstellen, entfernen oder modifizieren und Benutzern, Gruppen oder Containern Rollen zuweisen oder entziehen. Außerdem können die Rollenmitglieder damit einen Bericht für einen beliebigen Benutzer ausführen. Standardmäßig wird diese Rolle dem Benutzeranwendungsadministrator zugewiesen. Sie können diese Zuweisung nach dem Bereitstellen der Benutzeranwendung über die Seite *Verwaltung* > *Administratorzuweisung* in der Benutzeranwendung ändern. Während der Ausführung von „ConfigUpdate“ treten Änderungen an diesem Wert nur dann in Kraft, wenn Sie keinen gültigen Rollenadministrator beauftragt haben. Wenn ein gültiger Rollenadministrator existiert, werden Ihre Änderungen nicht gespeichert.
	Sicherheits-administrator	Diese Rolle bietet Mitgliedern die ganze Funktionspalette innerhalb der Sicherheitsdomäne. Der Sicherheitsadministrator kann für alle Objekte alle möglichen Aktionen innerhalb der Sicherheitsdomäne durchführen. Die Sicherheitsdomäne erlaubt es dem Sicherheitsadministrator, Zugriffsberechtigungen für alle Objekte in allen Domänen innerhalb des rollenbasierten Bereitstellungsmoduls zu konfigurieren. Der Sicherheitsadministrator kann Teams konfigurieren sowie Domänenadministratoren, beauftragte Administratoren und andere Sicherheitsadministratoren zuweisen. Sie können diese Zuweisung nach dem Bereitstellen der Benutzeranwendung über die Seite *Verwaltung* > *Administratorzuweisung* in der Benutzeranwendung ändern.
	Ressourcen-administrator	Diese Rolle bietet Mitgliedern die ganze Funktionspalette innerhalb der Ressourcendomäne. Der Ressourcenadministrator kann für alle Objekte alle möglichen Aktionen innerhalb der Ressourcendomäne durchführen. Sie können diese Zuweisung nach dem Bereitstellen der Benutzeranwendung über die Seite *Verwaltung* > *Administratorzuweisung* in der Benutzeranwendung ändern.

Einstellungstyp	Option	Beschreibung
	RBPM-Konfigurations-administrator	Diese Rolle bietet Mitgliedern die ganze Funktionspalette innerhalb der Konfigurationsdomäne. Der RBPM-Konfigurationsadministrator kann für alle Objekte alle möglichen Aktionen innerhalb der Konfigurationsdomäne durchführen. Der RBPM-Konfigurationsadministrator steuert den Zugriff auf Navigationselemente innerhalb des rollenbasierten Bereitstellungsmoduls. Außerdem konfiguriert der RBPM-Konfigurationsadministrator den Delegierungs- und Vertretungsservice, die Bereitstellungsbenutzerschnittstelle und die Workflow-Engine. Sie können diese Zuweisung nach dem Bereitstellen der Benutzeranwendung über die Seite *Verwaltung* > *Administratorzuweisung* in der Benutzeranwendung ändern.
	RBPM Reporting-Administrator	Zeigt auf den Reporting-Administrator. Das Installationsprogramm setzt diesen Wert standardmäßig auf denselben Benutzer wie die anderen Sicherheitsfelder.
	RBPM-Sicherheit neu initiieren	Kontrollkästchen zum Zurücksetzen der Sicherheit.
	IDMReport-URL	URL, die auf die Benutzeroberfläche des Identity-Berichterstellungsmoduls zeigt.

Einstellungstyp	Option	Beschreibung
Identitätsdepot-Benutzeridentität	*Benutzer-container-DN*	Erforderlich. Geben Sie den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten Namen des Benutzercontainers an. Benutzer in diesem Container (und unterhalb) dürfen sich bei der Benutzeranwendung anmelden. Sie können diese Einstellung nicht über „ConfigUpdate“ ändern, wenn Sie den Anwendungsserver gestartet haben, auf dem die Benutzeranwendung installiert ist. **Wichtig:** Stellen Sie sicher, dass der bei der Installation des Benutzeranwendungstreibers angegebene Benutzeranwendungsadministrator in diesem Container vorhanden ist, wenn dieser Benutzer Workflows ausführen können soll.
	Benutzercontainerbereich	Diese Angabe definiert den Suchbereich für Benutzer.
	Benutzerobjekt-klasse	Die LDAP-Benutzerobjektklasse (in der Regel inetOrgPerson).
	Anmeldeattribut	Das LDAP-Attribut (z. B. CN), das den Anmeldenamen des Benutzers repräsentiert.
	Benennungs-attribut	Das als ID verwendete LDAP-Attribut beim Nachschlagen von Benutzern oder Gruppen. Dieses Attribut ist nicht identisch mit dem Anmeldeattribut, das nur für die Anmeldung, nicht aber bei der Suche nach Benutzern oder Gruppen verwendet wird.
	Benutzermit-gliedschafts-attribut	Optional. Das LDAP-Attribut, das die Gruppenmitgliedschaft des Benutzers repräsentiert. Der Name darf keine Leerzeichen enthalten.

Einstellungstyp	Option	Beschreibung
Identitätsdepot-Benutzergruppen	*Gruppencontainer-DN*	Erforderlich. Geben Sie den eindeutigen LDAP-Namen (DN) oder den vollständig qualifizierten Namen des Gruppencontainers an. Wird von Entitätsdefinitionen innerhalb der Verzeichnisabstraktionsschicht verwendet. Sie können diese Einstellung nicht über „ConfigUpdate“ ändern, wenn Sie den Anwendungsserver gestartet haben, auf dem die Benutzeranwendung installiert ist.
	Gruppencontainerbereich	Diese Angabe definiert den Suchbereich für Gruppen.
	Gruppenobjektklasse	Die Objektklasse für die LDAP-Gruppen (in der Regel groupofNames).
	Gruppenmitgliedschaftsattribut	Das Attribut, das die Gruppenmitgliedschaft des Benutzers repräsentiert. Der Name darf keine Leerzeichen enthalten.
	Dynamische Gruppen verwenden	Wählen Sie diese Option, wenn Sie dynamische Gruppen verwenden möchten.
	Klasse für dynamisches Gruppenobjekt	Die Objektklasse für die dynamische Gruppe (in der Regel dynamicGroup).
Identitätsdepot-Zertifikate	*Keystore-Pfad*	Erforderlich. Geben Sie den vollständigen Pfad zur Keystore-Datei (`cacerts`) der JRE an, die der Anwendungsserver für die Ausführung verwendet, oder klicken Sie auf die kleine Browser-Schaltfläche und navigieren Sie zur `cacerts` -Datei. Während der Installation der Benutzeranwendung wird die Keystore-Datei geändert. Unter Linux oder Solaris benötigt der Benutzer eine entsprechende Berechtigung zum Schreiben in diese Datei. **Hinweis zu WebSphere.** Das Feld für den Keystore-Pfad muss auf das Installationsverzeichnis des RBPMs gesetzt werden, nicht auf den Speicherort der JDK-cacerts-Datei wie bei JBoss-Installationen. Der Standardwert ist auf den richtigen Speicherort gesetzt.
	Keystore-Passwort	Erforderlich. Geben Sie das `cacerts`-Passwort an. Die Vorgabe ist `changeit`.
	Keystore-Passwort bestätigen	

Einstellungstyp	Option	Beschreibung
Speicher für Herkunftsverbürgungsschlüssel	*Pfad für Herkunftsverbürgungsspeicher*	Der Speicher für Herkunftsverbürgungsschlüssel enthält alle verbürgten Zertifikate der Signierer. Wurde kein Pfad angegeben, ruft die Benutzeranwendung den Pfad von der Systemeigenschaft `javax.net.ssl.trustStore` ab. Wurde kein Pfad angegeben, wird `jre/lib/security/cacerts` verwendet.
	Passwort für Herkunftsverbürgungsspeicher	Wurde kein Passwort angegeben, ruft die Benutzeranwendung das Passwort von der Systemeigenschaft `javax.net.ssl.trustStorePassword` ab. Ist dort kein Wert angegeben, lautet das Passwort `changeit`. Dieses Passwort ist mit dem Master-Schlüssel verschlüsselt.
	Keystore-Typ JKS	Gibt den Typ der von Ihnen bevorzugten Digitalsignatur an. Wenn dieses Feld aktiviert ist, ist der Pfad für den Herkunftsverbürgungsspeicher vom Typ „JKS“.
	Keystore-Typ PKCS12	Gibt den Typ der von Ihnen bevorzugten Digitalsignatur an. Wenn dieses Feld aktiviert ist, ist der Pfad für denHerkunftsverbürgungsspeicher vom Typ „PKCS12“.
Novell Audit-Digitalsignatur-Zertifikat und Schlüssel		Enthält den Digitalsignaturschlüssel und das -zertifikat für den Audit-Service.
	Novell Audit-Digitalsignatur-Zertifikat	Zeigt das Digitalsignaturzertifikat für den Audit-Service an.
	Privater Schlüssel für Novell Audit-Digitalsignatur	Zeigt den privaten Schlüssel für die Digitalsignatur an. Dieser Schlüssel ist mit dem Master-Schlüssel verschlüsselt.
Access Manager-Einstellungen	*Gleichzeitige Abmeldung aktiviert*	Bei Auswahl dieser Option unterstützt die Benutzeranwendung die gleichzeitige Abmeldung von der Benutzeranwendung und dem Novell Access Manager bzw. iChain. Bei der Abmeldung leitet die Benutzeranwendung den Benutzer bei Vorhandensein des iChain- oder Novell Access Manager-Cookies zur ICS-Abmeldungsseite um.
	Seite 'Gleichzeitige Abmeldung'	Die URL für die Abmeldeseite von Novell Access Manager oder iChain, wobei die URL ein Hostname ist, den Novell Access Manager oder iChain erwartet. Wenn die ICS-Protokollierung aktiviert ist und sich ein Benutzer von der Benutzeranwendung abmeldet, wird der Benutzer auf diese Seite umgeleitet.

Einstellungstyp	Option	Beschreibung
Email-Serverkonfiguration	*Benachrichtigungsschablone HOST*	Geben Sie den Anwendungsserver an, der die Identity Manager-Benutzeranwendung . Beispiel: `myapplication serverServer` Dieser Wert ersetzt das $HOST$-Token in Email-Schablonen. Die erstellte URL ist eine Verknüpfung zu Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen.
	Benachrichtigungsschablone PORT	Ersetzt das $PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungsaufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
	für den sicheren Port der Benachrichtigungsschablone	Ersetzt das $SECURE_PORT$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
	Benachrichtigungsschablone PROTOCOL	Bezieht sich auf ein nicht sicheres Protokoll, HTTP. Ersetzt das $PROTOCOL$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
	für das sichere Protokoll der Benachrichtigungsschablone	Bezieht sich auf ein sicheres Protokoll, HTTPS. Ersetzt das $SECURE_PROTOCOL$-Token in Email-Schablonen, die für Bereitstellungsanforderungs-Aufgaben und Benachrichtigungen über Bereitstellungsgenehmigungen verwendet werden.
	Benachrichtigungs-SMTP-Email von:	Geben Sie Emails an, die von einem Benutzer in der Bereitstellungs-Email stammen.
	SMTP-Servername:	Geben Sie den SMTP-Email-Host für die Bereitstellungs-Email an. Dies kann eine IP-Adresse oder ein DNS-Name sein.

Einstellungstyp	Option	Beschreibung
Passwortverwaltung		
	Externe WAR-Datei für Passwort verwenden	Mithilfe dieser Funktion können Sie eine Seite „Passwort vergessen“ in einer externen WAR-Datei „Passwort vergessen“ sowie eine URL angeben, die die externe WAR-Datei „Passwort vergessen“ für den Rückruf der Benutzeranwendung über einen Webservice verwendet. Wenn Sie *Externe WAR-Datei für Passwort verwenden* auswählen, müssen Sie Werte für *'Passwort vergessen'-Link*, *Link zurück zu 'Passwort vergessen'* und *Webservice-URL zu 'Passwort vergessen'* angeben. Wenn *Externe WAR-Datei für Passwort verwenden* nicht aktiviert ist, verwendet IDM die interne Standardfunktion zur Passwortverwaltung. `/jsps/pwdmgt/ForgotPassword.jsp` (ohne http[s] am Anfang). Hierdurch wird der Benutzer nicht zu einer externen WAR-Datei, sondern zur in der Benutzeranwendung integrierten Funktionalität „Passwort vergessen“ umgeleitet.
	'Passwort vergessen'-Link	Diese URL verweist auf die Funktionsseite „Passwort vergessen“. Geben Sie eine `ForgotPassword.jsp`-Datei an, die sich in einer externen oder in einer internen WAR-Datei für die Passwortverwaltung befindet.
	Link zurück zu 'Passwort vergessen'	Geben Sie den *Link zurück zu 'Passwort vergessen'* an, den der Benutzer nach Durchführung eines „Passwort vergessen“-Vorgangs anklicken kann.
	Webservice-URL zu 'Passwort vergessen'	Dies ist die URL, die die externe WAR-Datei für „Passwort vergessen“ verwendet, um die Benutzeranwendung zum Durchführen von Kernfunktionen von „Passwort vergessen“ aufzurufen. Das Format der URL ist: `https://<idmhost>:<sslport>/<idm>/pwdmgt/service`
Sonstige	*Sitzungszeit-überschreitung*	Die Sitzungszeitüberschreitung der Anwendung.
	OCSP-URI	Wenn für die Client-Installation das OSCP (On-Line Certificate Status Protocol) verwendet wird, stellen Sie eine URI (Uniform Resource Identifier) bereit. Beispiel für das Format: http://host:port/ocspLocal. Die OCSP-URI aktualisiert den Status der verbürgten Zertifikate online.
	Konfigurations-pfad für Autorisierung	Vollständig qualifizierter Name der Konfigurationsdatei für die Autorisierung.

Einstellungstyp	Option	Beschreibung
	Identitätsdepot-index erstellen	Wählen Sie dieses Kontrollkästchen aus, wenn das Installationsprogramm Indizes für die Attribute „manager“, „ismanager“ und „srvprvUUID“ erstellen soll. Sind für diese Attribute keine Indizes vorhanden, kann dies insbesondere in einer Cluster-Umgebung eine eingeschränkte Leistung der Benutzeranwendung zur Folge haben. Sie können diese Indizes manuell mithilfe des iManager erstellen, nachdem Sie die Benutzeranwendung installiert haben. Weitere Informationen hierzu finden Sie unter Abschnitt 9.3.1, „Erstellen von Indizes in eDirectory“, auf Seite 150. Zur Erzielung einer optimalen Leistung sollte die Erstellung des Index abgeschlossen sein. Die Indizes sollten sich im Online-Modus befinden, bevor Sie die Benutzeranwendung verfügbar machen.
	Identitätsdepot-index entfernen	Entfernt Indizes von den Attributen „manager“, „ismanager“ und „srvprvUUID“.
	Server-DN	Wählen Sie den eDirectory-Server aus, auf dem die Indizes erstellt oder entfernt werden sollen. **Hinweis:** Zum Konfigurieren der Indizes auf mehreren eDirectory-Servern müssen Sie das Dienstprogramm „ConfigUpdate“ mehrmals aufrufen. Es kann jeweils nur ein Server angegeben werden.
Containerobjekt	*Ausgewählt*	Wählen Sie alle zu verwendenden Containerobjekttypen aus.
	Container-objekttyp	Wählen Sie die Typen aus den folgenden Standard-Containern aus: Standort-, Länder-, Organisationseinheits-, Organisations- und Domänenobjekte. Sie können in iManager auch eigene Container erstellen und mithilfe der Option *Neues Containerobjekt hinzufügen* hinzufügen.
	Container-attributname	Listet den mit dem Containerobjekttyp verknüpften Attributnamen auf.
	Neues Containerobjekt hinzufügen: Container-objekttyp	Geben Sie den LDAP-Namen einer Objektklasse aus dem Identitätsdepot an, die als Container dienen kann.
	Neues Containerobjekt hinzufügen: Container-attributname	Geben Sie den Attributnamen des Containerobjekts an.